A CRITIQUE OF CYBERCRIME AND THE LAW: CHALLENGES AND THE WAY FORWARD

BY

AGBONMENLO, Samuel Iroseyike
PG/LAW/230036

FACULTY OF LAW
BENSON IDAHOSA UNIVERSITY
BENIN CITY, EDO STATE, NIGERIA.

APRIL, 2024

A CRITIQUE OF CYBERCRIME AND THE LAW: CHALLENGES AND THE WAY FORWARD

BY

AGBONMENLO, Samuel Iroseyike
PG/LAW/230036

A DISSERTATION SUBMITTED TO THE FACULTY OF LAW, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF LAWS (LL.M) OF BENSON IDAHOSA UNIVERSITY, BENIN CITY, EDO STATE, NIGERIA

APRIL, 2024

CERTIFICATION

I, **AGBONMENLO, Samuel Iroseyike,** with Matriculation No. **PG/LAW/230036** hereby certify that, the entire work in this dissertation is the product of my personal research, all sources used and referred to have been duly acknowledged, and this dissertation has neither in whole nor in part been presented for another degree elsewhere.

_____ _____

AGBONMENLO, Samuel Iroseyike **Date**

APPROVAL

We certify that **AGBONMENLO, Samuel Iroseyike** with Matriculation Number **PG/LAW/230036** completed this dissertation in partial fulfillment of the requirements for the award of Master of Laws Degree (LL.M) of Benson Idahosa University.

_____ _____

Prof. (Mrs.) T. U. Akpoghome Date
Supervisor

_____ _____

Dr. T. C. Nwano Date
Ag. Head of Department (Public Law)

_____ _____

Dr. (Mrs.) S. O. Idehen Date
Ag. Dean, Faculty of Law

_____ _____

Internal Examiner Date

DEDICATION

This research work is foremost dedicated to the Supreme Being, the Almighty God who made me seised of the fact that in every calamity, he creates oasis of hope, strength and comfort. Next to the fond memories of my parents His Eminence Pa Isaac Eriarevbe Agbonmenlo and Mrs. Maria Agbonmenlo (both late) who laid the foundation for all I have achieved so far and to my treasured wife and kids who has inspired me to be the best of myself.

ACKNOWLEDGMENTS

It has indeed been a turbulent moment traipsing through these dark alleys of this intellectual voyage. But in reminiscence of the comforting words of the psalmist “Thank to the Almighty God, who has not made us, (nay me) prey to the teeth of the adversary.” I am infinitely grateful to Him for the gift of life, His mercies, provision and for not allowing me fall prey to the deadly fangs of detractors, this misty one year.

My unquantifiable gratitude goes to Prof. (Mrs.) T. U. Akpoghome (my inimitable IHL Lecturer and adept Dissertation Supervisor). I would not have achieved the mileage of success gained during this research work save for her dedication and painstaking work towards the supervision. Passing through her academically will forever etched in my memory, a flame that burns eternal. Many thanks, for your inestimable guidance, intelligent corrections and thoroughness. I doff my hat ma.

I wish to acknowledge and appreciate the Ag. Dean Faculty of Law Dr. (Mrs.) S. O. Idehen, the LL.M Program Co-coordinator, Dr. T. C. Nwano, my other invaluable lecturers; Dr. J. M. Ekwe, Dr. E. Akhigbe for their lectures in different areas of law which have impacted a life time knowledge in me. More grease to elbows sirs.

It is heartwarming at this point to express my deep and unwavering gratefulness to my treasured wife Dr. (Mrs.) Annabella Agbonmenlo for her support and for exposing me to a vista of endless possibilities in this world since the inception of our union. I cherish you and to our cherished kids, I say thanks for being there.

I would like to express my profound gratitude to my spiritual fathers, the General Overseer of the Mountain of Fire and Miracle Ministries Dr. D. K. Olukoya and Pastor Nwanadile Olisaemeka. the Regional Overseer, Region xii Aduwawa, Benin City for their life sustaining prayers. To my one and only brother Barr. Peterson Agbonmenlo you have my gratitude for your support and counselling. To all my fellow LL.M students, 2023 set and others too numerous to mention, my success story cannot be told without you, God bless you all.

TABLE OF CONTENTS

CONTENT PAGES

Cover Page - - - - - - - - - - i

Title Page - - - - - - - - - - ii

Certification - - - - - - - - - - iii

Approval - - - - - - - - - - iv

Dedication - - - - - - - - - - v

Acknowledgment - - - - - - - - - vi

Table of Contents - - - - - - - - - vii

Table of Statues - - - - - - - - - x

Table of Cases - - - - - - - - - xiv

Table of Abbreviations - - - - - - - - xv

Abstract - - - - - - - - - - xvi

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study - - - - - - - 1

1.2 Statement of the Problem - - - - - - - 4

1.3 Aim and Objectives of the Study - - - - - - 7

1.4 Scope and Limitation of the Study - - - - - - 7

1.5 Significance of the Study - - - - - - - 8

1.6 Research Methodology - - - - - - - 9

1.7 Chapter Analysis - - - - - - - - 10

CHAPTER TWO
CONCEPTUAL THEORITICAL FRAMEWORKS AND LITERATURE REVIEW

2.1. Conceptual Clarifications - - - - - - 12

2.1.1 Concept of Crime - - - - - - - - - 12

2.1.2 Concept of Cybercrime - - - - - - - 14

2.1.3 Concept of Cyber Security - - - - - - - 18

2.1.4 Concept of Internet - - - - - - - 20

2.1.5 Concept of Organized Crime - - - - - - 22

2.2. Theoretical and Historical Foundations - - - - - 25

2.2.1. Biological Theory of Crime - - - - - - - - 25

2.2.2. Classical Theory of Crime - - - - - - - - 27

2.2.3. Psychological Theory of Crime - - - - - - - 28

2.2.4. Sociological Theory of Crime - - - - - - - 32

2.3. Literature Review - - - - - - - - 36

2.4. Discussion on the Gaps - - - - - - - 43

CHAPTER THREE
CYBERCRIME IN NIGERIA: TYPOLOGIES, CAUSES AND EFFECTS

3.1. Foundation to the History of Cybercrime in Nigeria - - - - 44

3.1.1. History of Cybercrime in Nigeria - - - - - - - 45

3.2 Classification of Cybercrime - - - - - - - 46

3.2.1 Classification by Subject - - - - - - - - 47

3.2.2 Classification by Object - - - - - - - - 48

3.2.3 Classification by Structural Organization - - - - - - 49

3.2.4 Classification by Victimology - - - - - - - 50

3.3. Typologies of Cyber Crime in Nigeria - - - - - - 51

3.4. Causes of Cyber Crime in Nigeria - - - - - - - 61

3.5. Effect of Cyber Crime in Nigeria - - - - - - - 67

CHAPTER FOUR
LEGAL AND INSTITUTIONAL FRAMEWORKS FOR CONTROL AND PREVENTION CYBERCRIME IN NIGERIA

4.1. Legal Foundation for Control and Prevention of Cybercrime in Nigeria - 73

4.2 Domestic Legal Frameworks for the Prevention and Control Cybercrime in Nigeria - - - - - - 74

4.2.1 The Nigeria Criminal Code Act 2004 - - - - - 74

4.2.2 The Economic and Financial Crime Commission Act, 2004 - - - 76

4.2.3 Advance Fee Fraud and other Fraud Related Offences Act 2006 - - 80

4.2.4 Child's Rights Act 2003 - - - - - - - 82

4.2.5 Copyright Act 2022 - - - - - - - - 83

4.2.6. The Cybercrimes (Prohibition, Prevention, ETC) Act, 2015 - - - 84

4.3. Institutional and Regulatory Frameworks for Prevention and Control of Cyber Crime in Nigeria - - - - - - - - 95

4.4. Challenges in Cybercrime Investigation, Prevention and Control in Nigeria 97

4.5. Approaches of other Jurisdictions towards Prevention and Control of Cyber Crime - - - - - - - - - - 106

4.6. International Framework for Prevention and Control of Cyber Crime - 111

4.6.1 United Nations Office on Drugs and Crimes - - - - - 111

4.6.2 Council of Europe Convention on Cybercrime - - - - 111

4.6.3 ECOWAS Directive on Cybercrime - - - - - - 112

4.6.4. African Union Convention on Cyber Security and Personal Data Protection 113

CHAPTER FIVE
CONCLUSION

5.1. Summary of Finding - - - - - - - - 115

5.2. Recommendations - - - - - - - - - 118

5.3. Contribution to knowledge - - - - - - - 123

5.4. Areas for Further Studies - - - - - - - 124

5.5. Conclusion - - - - - - - - - 124

Bibliography - - - - - - - - 127

TABLE OF STATUTES

FOREIGN

African Charter on the Rights and Welfare of the Child

Articles 1 - - - - - - - - - - 82

Articles 2 - - - - - - - - - - 82

African Union Convention on Cyber Security and Personal Data Protection 2014

Articles 2 - - - - - - - - - - 113

Articles 8 - - - - - - - - - - 113

Articles 24 - - - - - - - - - - 113

Articles 25 - - - - - - - - - - 113

Articles 26 - - - - - - - - - - 113

Council of Europe Convention on Cybercrime 2001

Preamble to the Convention - - - - - - - - 111

United Nations Convention against Transnational Crime

Article 2 - - - - - - - - - - 22

LOCAL

Advance Fee Fraud and Related Offences Act, 2006

Section 1 - - - - - - - - - - 80

Section 1 - - - - - - - - - - 81

Section 12 - - - - - - - - - - 81

Section 13 - - - - - - - - - - 81

Section 20 - - - - - - - - - - 81

Child Rights Act, 2003

Section 1 - - - - - - - - - - 82

Section 30 - - - - - - - - - - 82

Section 35 - - - - - - - - - - 82

Constitution of the Federal Republic of Nigeria 1999 as amended

Section 4 - - - - - - - - - - 99

Section 36 - - - - - - - - - - 65

Section 174 - - - - - - - - - - 103

Section 211 - - - - - - - - - - 103

Copyright Act, 2022

Sections 1 - - - - - - - - - - 83

Section 38 - - - - - - - - - - 83

Section 38 - - - - - - - - - - 84

Section 44 - - - - - - - - - - 83

Section 44 - - - - - - - - - - 84

Cybercrimes (Prohibition, Prevention ETC) Act 2015

Section 1 - - - - - - - - - 85

Section 2 - - - - - - - - - - 85

Section 3 - - - - - - - - - - 86

Section 5 - - - - - - - - - - 87

Section 6 - - - - - - - - - - 88

Section 7 - - - - - - - - - - 98

Section 8 - - - - - - - - - - 89

Sections 9 - - - - - - - - - - 89

Section 10 - - - - - - - - - - 89

Section 11 - - - - - - - - - - 89

Section 12 - - - - - - - - - - 89

Section 13 - - - - - - - - - - 90

Section 14 - - - - - - - - - - 90

Section 15 - - - - - - - - - - 90

Section 16 - - - - - - - - - - 90

Section 17 - - - - - - - - - - 90

Section 18 - - - - - - - - - - 90

Section 22 - - - - - - - - - - 90

Section 22 - - - - - - - - - - 91

Section 23 - - - - - - - - - - 91

Section 24 - - - - - - - - - - 92

Section 25 - - - - - - - - - - 92

Section 25 - - - - - - - - - - 93

Section 26 - - - - - - - - - - 93

Section 26 - - - - - - - - - - 94

Section 27 - - - - - - - - - - 94

Section 27 - - - - - - - - - - 95

Section 41 - - - - - - - - - - 95

Section 42 - - - - - - - - - - 85

Section 42 - - - - - - - - - - 96

Section 43 - - - - - - - - - - 96

Section 44 - - - - - - - - - - 85

Section 45 - - - - - - - - - - 97

Section 47 - - - - - - - - - - 97

Section 47 - - - - - - - - - - 103

Section 50 - - - - - - - - - - 104

Section 58 - - - - - - - - - - 96

Economic and Financial Crime Commission Act, 2004

Section 6 - - - - - - - - - - 77

Section 7 - - - - - - - - - - 76

Section 7 - - - - - - - - - - 79

Section 7 - - - - - - - - - - 80

Section 7 - - - - - - - - - - 104

Section 13 - - - - - - - - - - 79

Section 13 - - - - - - - - - - 104

Section 46 - - - - - - - - - - 76

Nigeria Criminal Code Act, 2004

Sections 383 - - - - - - - - - - 74

Section 418 - - - - - - - - - - 75

Section 419 - - - - - - - - - - 74

Section 419 - - - - - - - - - - 75

Nigeria Police Force Act, 2020

Sections 4 - - - - - - - - - - 99

Section 66 - - - - - - - - - - 104

TABLE OF CASES

Ezekiel v. Attorney-General of the Federation (2017) Vol. 266 LRCN 1 - - 103

Madukolu v. Nkemdilim (1962) 2 SCNLR 34 - - - - - 103

Shema v. Federal Republic of Nigeria (2018) NWLR Pt. 1624 at 337 - - 104

TABLE OF ABBREVIATIONS

AI	Artificial Intelligence
ATM	Automated Teller Machine
BVN	Bank Verification Number
CETAP	Cybersecurity Education and Training Assistance Program
CISA	Cybersecurity and Infrastructure Security Agency's (CISA)
COE	Council of Europe
DBS	Disclosure Barring Service
DAT	Data and Airtime Time
DOS	Denial of Service Attacks
EFCC	Economic and Financial Crime Commission
FBI	Federal Bureau of Investigation
ICT	Information and Communications Technology
IP	Internet Protocol
NDIC	Nigerian Deposit Insurance Corporation
NGO	Non-Governmental Organization
SACCWG	Strategic Alliance Cyber Crime Working Group
TCP	Transmission Control Protocol
UNGA	United Nations General Assembly
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNESCO	United Nations Educational, Scientific and Cultural Organization
USD	United States Dollars

ABSTRACT

The domains of modern activities have extended beyond the turfs of land, sea, air and space to include the cyberspace. The advancement in technology has gained universal acceptance which has made the use of computer system and the internet almost unavoidable in today's world. Most of the facets of all human activities which include but not limited to; banking, health, commercial, media, education, entertainment, religion etc. are now internet based. However, this progressive and welcoming development of the internet has also come with its adverse effect due to the growing rate of internet-related crimes called 'cybercrime' that takes place in cyberspace where criminal activities have progressed almost unhindered. It is the existence of the high rate of criminality in the cyberspace that led to this research. The research examines the legal frameworks on the subject matter adopting the doctrinal methodology. The research finds that the increasing rate of cybercrime in Nigeria has been linked with weak or non-existent legal and regulatory frameworks on cybercrime and cyber security, failure of the relevant law enforcement agencies to implement the existing laws which are to prevent and combat the challenges posed by this crime in Nigeria. The research also finds that the high rate of educated youth unemployment, contribute to the menace and must be addressed headlong. A careful examination of these laws also shows that there are gaps that needs to be filled if the battle against cybercrime is to be won and this research has been significant in this regard. This research, therefore attempts to proffer bridges to these gaps. Based on the findings, the research recommends the frequent review of legislations to keep abreast with the dynamics of cyberspace and cybercrime. It further recommends that information technology professionals be involved at the law-making process so as to help make laws that would be in line with the extant level of technology, training of law enforcement agencies, recruitment of skilled personnel, engagement of expert in prosecution of cybercrimes, online reporting system of cybercrime, public enlightenment, international cooperation, poverty alleviation and employment generation among host of others. Following the recommendations, the research concludes that, if holistically implemented, will be recipe for preventing and combating the menace of cybercrime in Nigeria.

CHAPTER ONE
INTRODUCTION

1.1. Background of the Study

The advent of globalization facilitated by information and communication technology (ICT) launched Nigeria into the 21st century. As a consequence, Nigeria's socio-cultural space today is one where local events are being shaped by external forces at varied spheres. The advancement in technology has gained universal acceptance which has made the use of computer system and the internet almost unavoidable in today's world. Computer has come to be a close assistant to man. With the advent of internet, the world has become a global village and all the erstwhile barriers that seem to barricade some territories from others have collapsed. The world through internet has, indeed become a global community.[1] The introduction of the internet offers great advantages and opportunities especially for developing countries. ICT related applications such as 'e-government, e-commerce, e-banking, e-education, e-health, e-entertainment, e-environment etc. are seen as bolsters for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas.[2] The COVID 19 period saw the introduction and adoption of electronic judicial proceedings and it has gained ground now. Election petition judgments are now being delivered online[3]. E-conferences, workshops and seminars have equally evolved.

[1] F. B. Okeshola and A. K. Adeta, 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria' [2013] (3)(9*) American International Journal of Contemporary Research*, 98.
[2] M Gercke, 'Understanding Cybercrimse: Phenomena, Challenges and Legal Response' <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>. Accessed 20th November 2023.
[3] See the 2023 Nigerian Presidential Election Petition Tribunal proceedings where the court of Appeal and the Supreme Court live stream its proceedings and judgments across the world. Also accessed 20th November 2032 from <https://www.thecable.ng/what-next-after-tribunal-judgement-an-analysis-of-election-appeals-procedures-in-nigeria>.

Computer, together with information and communications technology (ICT) using the platform of the internet, has come to ease the way of doing business by eliminating most shortcomings and limitations of man especially the inability of man to be in more than a place at the same time. With the aid of a computer and ICT, a man can virtually be in more than one place at a time. Further, the cost of doing businesses including transportation cost has drastically been reduced owing to the employment of computer and the internet in businesses. Other business uncertainties and fears have been allayed. The array of armed robbery attacks which has been a bane to free movement of people and funds has equally been reduced with the use of online transfer of fund meaning that individuals do not have to travel long distances and physical cash need not to be carried from one location to another in order to consummate business transactions. In the banking sector, the use of ICT has provided assistance for facilitating seamless transactions. ICT has also facilitated import and export of goods and services. Long queues at the banks have been reduced by and through the use of Automated Teller Machines (ATM). In the healthcare sector also, advancement in the ICT has equally contributed in the improvement of healthcare services. Educational institutions are not left out as more information is made available and accessible with the advent of ICT on the platform of the internet.

The list of the advantages attendant to the use of computer together with the internet is inexhaustible. However, despite the amplitude of advantages attendant with the use of computer and the internet, there is an adverse effect. The adverse effect in this context is termed cybercrime. Cybercrime is a fast-growing expanse of crime whereby the internet has been used to commit a variety of criminal activities that knows no borders either physical or cybernetic,[4] thus laying credence to the saying that developments attract crime. Nearly every advancement

[4] Interpol on International Cybercrime. <www.interpol.int/Crime-areas/Cybercrime/Cybercrime>. [Accessed 20th November 2023].

in technology has been accompanied by a corresponding niche to be exploited for criminal purposes.[5] As with other aspects of globalization, its rapid expansion has far exceeded regulatory capacity, and this absence of regulatory framework has left space for many abuses. The problem is compounded by the fact that the internet was fashioned on a military system designed to circumvent interference and external controls. The computer and the internet has furthermore supplied a new natural environment for crime.[6] These internet crimes are usually enormous in their financial magnitude. For example, in 2003 alone, it was estimated that malicious software caused damages of up to USD 17 billion.[7] In a survey, nearly 60 per cent of businesses in the United States believe that cybercrime is more costly to them than physical crime.[8]

Nigeria as a country is not left behind in tapping into the advantages of the internet as the proliferation of the use of the internet continues to be on the increase among different age brackets of the population. It is estimated in a study that out of the total population of Nigeria of approximately 200 million, 122.5 million have access to internet services as at 31st January, 2023 Nigeria's internet penetration rate was 50.4%.[9] This number no doubt continues to grow exponentially and with this growth in the number of users of the internet comes with an attendant growth of the incidence of crime being committed by the use of the internet. Efforts to check the abuse occasioned by the use of the internet have however not been able to keep abreast with the spate of cybercrime in the country as several factors continue to exacerbate the incidences of the crime in the Nigeria.

---

[5] J. Clough, 'Principles of Cybercrime' (Cambridge University Press 2010), 112.
[6] A. Yassir and S. Nayak 'Cybercrime: A Threat to Network Security' [2012] (12) (2) *International Journal of Computer Science and Network Security*, 84.
[7] CRS Report for Congress on the Economic Impact of Cyber-Attacks. [2004] <www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf> Accessed 20th November 2023.
[8] IBM survey (published 2006). <www.03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html>. Accessed 20th November 2023.
[9] Internet World Statistics, Internet Users Statistic for Africa and Internet Penetration in Africa as at 31st January 2017 <www.internetwordstats.com/stats1.html>. Accessed 20th November 2023.

1.2. Statement of the Problem

As stated above, despite the enormous advantages associated with the use of computer and internet, the use is susceptible to abuse. One of such ways through which this abuse occurs is cybercrime. Like the rest of the world, the scourge of cybercrime has posed a negative and alarming threat to Nigeria in different sectors of her economy. Incidence of cybercrime continues to be on the increase with increase in the number of internet users in the country.

Despite the high number of the population that are exposed to the use of the internet, a significantly low number have the requisite knowledge and expertise to protect themselves from cybercrimes of all sorts.[10] Most internet users in the country who use same mostly for social media fall victim to identity theft, fraud, privacy invasion, account hack due to their lack of technical knowhow ranging from the worst category who are not aware of the existence of the activities of criminals making use of the internet to orchestrate crimes to those who despite being aware of the existence of cybercrime still do not know how to protect themselves.

Financial institutions in the country are not left out as they too are victims of cybercrimes. Most companies including banks do not have trained professionals that can withstand attacks by these internet criminals. Their systems and firewalls are not strong enough to withstand attacks by cybercriminals consequently, a lot of funds are lost annually to cybercrime. Due to the increase in the incidences of cybercrime, greater cost is involved in the running of different organizations in the country as allocation has to be made towards protecting each organization from cyber-attacks. Given the sophisticated training of these criminals, greater cost has to be expended in hiring the services of professionals with skill sets to match those possessed by cybercriminals. This is not without great cost.

[10] *Ibid.* (n1), 44-45.

Further, the educational sector of the country has witnessed incidences of cybercrimes being committed by students and outsiders alike. Due to the fact that most educational institutions have incorporated the use of internet in their administration, it has become easier for these cyber criminals to access institutions database and commit one form of criminal activity or the other. These ranges from falsification of certificates, alteration of results, falsification of admission, examination malpractices and a whole lot more. Beyond the attack on the institution, positive values which are one of the virtues to be taught in institutions of learning have continued to be eroded as the perpetrators of some of the resounding cybercrimes are students who continue to influence one another into their fold. Thus the incidences of cybercrime by students in our universities continue to be on the increase exponentially. Unemployment, low standard of living and poverty identified are some of the root causes for involvement of individuals in crime in general and cybercrime in particular has continued to thrive in the country. Most youths (especially graduates) in the country within employment age are either unemployed, seasonally employed or under employed affording them ample time and opportunity to engage in cybercrime. Low standard of living and poverty ravaging a significant number of the population has contributed in presenting cybercrime as a lucrative alternative to starving.

Corruption in government, embezzlement of public funds and misappropriation of common goods that continue to thrive in our political system with the perpetrators usually going unpunished has provided moral justification for the involvement by the average poor Nigerians in cybercrime. Most criminals who engage in this crime perceive themselves as doing what is right by stealing from those who stole from the public purse and who are seemingly beyond the reach of the law. Cybercrime especially as it relates to internet financial fraud then is perceived as a means of redistribution of wealth from dishonest political rich to the poor. The ease with which cybercrime can be committed and the relatively low cost of committing such

crimes in the country continue to aggravate the already bad situation. With the use of a computer including a cell phone that can access the internet, such crimes can be committed. Similarly, the fact that the crime can be committed remotely with less prospect of being caught seems to boost the attractiveness of this crime to prospective criminals. Thus, from the comfort of one's home and with the use of legitimate devices one can conveniently engage in cybercrime with little or no risk of being caught in the web of the law. Due to the multitude of crimes that can be committed using the internet, there is no comprehensive legal regime that will absolutely proscribe cybercrime in its entirety. Most legislative concerns and attentions are directed towards the enactment of laws that deal with financial aspects of these crimes thereby neglecting other grievous facets of cybercrime such as identity theft which has a much damaging effect as the financial aspect of cybercrime.

Lack of technical knowhow to match those possessed by cybercriminals has continued to militate against activities and operations of security agencies in the country in combating the offence. Most security outfits in the country are themselves victims of cybercrime as their systems are not sophisticated enough to withstand or combat attacks by cybercriminals. Lack of sophisticated systems, trained personnel, secured connections by these security outfits all contribute to the weak front posed against the scourge of cybercrime in the country. With the exponential increase in the incidences of cybercrime in Nigeria, the reputation and integrity of the country in the international community continues to wane culminating in most citizens of other countries always being weary and wavering to engage in business activities over internet with Nigerians as they are afraid of falling victim to cybercriminals in the country. Trust is an essential motivator in business, the absence of which adversely affects and militates against business transactions, the situation in the country has adversely affected the economy as Nigerians are perceived not to be trustworthy. The foregoing statement of the problem prompts the conduct of this research work.

In the light of the above statement of the problem, the following research questions are hereby formulated:

1. What are the types of cybercrime in Nigeria and the root causes for the commission of same?
2. What are the legal and institutional frameworks for the controlling and combatting of cybercrime in Nigeria?

1.3. Aim and Objectives of the Study

The primary aim of this research is to critique the law on cybercrime, identify the challenges and way forward in the prevention and control of cybercrime in Nigeria. Towards realizing this aim, the following are the objectives of this research work:

1. To discover the extent and types of cybercrime committed in Nigeria
2. To examine the root causes for the commission of cybercrime and the attendant challenges.
3. To analyze the extant legal regime and institutional frameworks proscribing cybercrime in Nigeria.
4. To review the role of different security agencies towards the prevention and control of cybercrime in Nigeria
5. To recommend strategies for preventing and combating cybercrime in Nigeria

1.4. Scope and Limitation of the Study

As technological advancements are a trans-cultural phenomenon and not the exclusive preserve of any particular culture, so also is it with cybercrime which is not a threat confined along the line of national territories. Cybercrime is a threat that is affecting the comity of nations of the world in different graduation and appearances. As varied as the threat is, so also is the

multifaceted approach adopted towards combating same by different nations of the world depending on the typology prevalent and peculiar in each such jurisdiction. This research work focuses on the menace of cybercrime as it is exhibited in Nigeria as a nation as well as the strategies and approaches towards its prevention and control in Nigeria. Cursory references however will be made to other technologically savvied jurisdictions in order to glean some lessons and approaches adopted in combating cybercrime. This research work is majorly limited by; lack of fund, time constraint and non-availability of text couple with shortage of judicial decisions (case law) in the area of cybercrime, being an emerging area of law in the Nigerian legal system.

1.5. Significance of the Study

Following the recognition that the internet is not amenable to positive use only but is equally susceptible to abuse by its users and given the extent and gravity of damage that can result from cybercrime, nations have continued to devise approaches and strategies of combating the scourge and attendant challenges of cybercrime. In view of the undeniable fact that Nigeria is not immune to cybercrime, it is imperative to conduct this research. This research is therefore significant as its findings provide:

1. Information on the relevant rules on cybercrime;
2. Data on the root causes driving the involvement of individuals in the commission of cybercrime, the methodology adopted by cybercriminals in perpetrating the crime;
3. Insight into the existing patterns, typology of cybercrime in Nigeria and other jurisdictions;
4. Information on the challenges for prosecuting cyber offenses in Nigeria etc.

1.6. Research Methodology

The term 'research methodology' refers to a way to systematically solve a research problem. It may be understood as a 'science of studying how research is done scientifically'. It involves the study of various steps and methods that a researcher needs generally adopt in his investigation of a research problem along with the logic behind them. It is a study of not only of the methods but also of explanation and justification for using certain research methods and of the methods themselves[11]. It includes in it the philosophy and practice of the whole research process. In other words, research methodology is a set of rules of procedures about the way of conducting research. C.R. Kothari,[12] noted thus:

> *...when we talk of research methodology we not only talk of the research methods but also consider the logic behind the methods we us in the context of our research study and explain why we are using a particular method or technique and why we are not using others so that research results are capable of being evaluated either by the researcher himself or by others, why a research study has been undertaken, how the research problem has been identified, in what way and why the hypothesis has been formulated, what data have been collated and what particular methods has been used and a host of similar other questions are usually answered when we talk of research methodology concerning a research problem or study.*[13]

There are two major methods of obtaining empirical data in legal research and they are: the doctrinal and non-doctrinal methods[14]. The doctrinal method that is commonly adopted in legal research entails gathering of relevant legal materials on the chosen topic and carrying out critical analysis of the data. The non-doctrinal method on the other hand, is generally used

[11] MOU Gasiokwu, Legal Research Methodology and Project Writing (Jos – Nigeria; Fab Education Books, 1994)
[12] K. R. Kathari, Research Methodology: Methods and Techniques (New Age International Publishers, New Delhi, 2nd ed., 2001, Reprint 2007), 2.
[13] *Ibid*, 2.
[14] T. U. Akpoghome, O. T. Umahi and T. C. Nwano. Mapping the Contours of Legal Research Writing and Documentation in Nigeria (University of Nigeria Press Ltd 2nd ed. 2020), 47.

among scientists and social scientists to conduct researches using empirical techniques like interviews, questionnaires, observation, experimental designs and statistical analysis

This research, being a legal research into law as a normative science, statutory provisions, doctrines, concepts, case law and the assemblage of relevant legal materials, the doctrinal methodology will be best suited for this study. References will be made to primary sources including; statute books, rules, conventions, and judicial authorities as well as to secondary sources including; books, articles in learned journals, reports and treaties. Reliance will also be placed on internet resources. Relevant materials including laws accessed from these sources will be collated, examined and analyzed towards achieving the aim and objectives of this research work.

1.7. Chapter Analysis

This research is divided into five chapters which are divided into heads and sub-heads.

Chapter One deals with the introduction of the research topic and will avail the reader the general scope of the research work and serves as a study map.

Chapter Two examines the conceptual clarifications by attempting to give meanings and definitions to words and terms in this research work. The chapter further analyzes the various theories underlying the rationale behind individual engagement in criminal activities as well as clarifying some concept peculiar to the discourse on cybercrime which will be reoccurring in the course of this work. It examines the existing literature in order to discover the existing gaps and use same to drive the current research.

Chapter Three analyzes the types of cybercrime in Nigeria and the root causes for the commission of same.

Chapter Four dwells on the legal and institutional framework put in place towards preventing and combating the challenges of cybercrime in Nigeria and international legal regime on cybercrime will equally be looked at

Chapter Five contains the summary of findings, recommendations, contribution to knowledge, areas for further research and conclusion.

CHAPTER TWO
CONCEPTUAL THEORITICAL FRAMEWORKS AND LITERATURE REVIEW

2.1. Conceptual Clarifications

Crime is a complex phenomenon that is dynamic differing amongst cultural lines and changing with time. As such what is considered a crime in one culture and at one time may not be so considered in another clime and at different times. Hence, there cannot be a simple explanation of the underlying factor behind the commission of crime by individuals. This chapter is concerned with clarifying some concept peculiar to the discourse on cybercrime and which will be reoccurring in the course of this research work as well as analyzing the various theories underlying the rationale for engagement by individuals in criminal activities.

2.1.1. Concept of Crime

The word "crime" is a common term used often by different individuals in the society. However, as noted by Morrsion,[1] although "crime" seems like a common sense category, this is only a superficial appearance as there is a practical and scholarly problem of understanding what constitutes a crime. This problem arises from the fact that "crime" is a complex interaction of many processes: from the creation of a concept of "crime", to people identifying some event as a crime; from the responses to the event so called, to the behaviour and formal activities of state agencies (or in the emerging global arena supra-national bodies such as the International Criminal Court or the International Criminal Tribunal for Yugoslavia) that may or may not process the persons responsible as "criminals" and punish them.

Crime as with most concepts cannot be easily and comprehensively defined. This is because what constitute a crime usually differs in both time and climes. In other words, what amount to crime is dependent on definition given to it in a particular geographical territory and at a

[1] W. Morrison, Criminology: Civilization and the New World Order (Routledge Publisher London, 2006).

particular time. What is considered as a crime in one territory may not be so considered in another territory. Equally, what is considered as a crime in a given period of time may not be considered as a crime at other times.

Thus, the conceptions of crime vary so widely from culture to culture and changes with time to such an extent that it is extremely difficult to name any specific act universally regarded as criminal.[2] This prompted McCabe[3] to assert that "there is no word in the whole lexicon of legal and criminological terms which is so elusive of definition as the word 'crime'". Generally, a crime involves the idea of public as opposed to private wrong. Crime can be defined as any act or omissions forbidden by law and can be punished by imprisonment or fine. Several scholars have attempts to confer a definitive formula to the term "crime".

Glanville Williams, for example, defined crime as "an act that is capable of being followed by criminal proceedings, having one of the types of outcomes (punishment etc.) known to follow these proceedings".[4] Tappan defined crime as "an intentional act or omission in violation of criminal law (statutory and case law), committed without defence or justification and sanctioned by the State as a felony or misdemeanor".[5]

Further, the Waverly Encyclopedia[6] defines it as, "An act forbidden by law and for performing which the perpetrator is liable to punishment". Halsbury[7] defines crime as, "an unlawful act or default, which is an offence against the public and which renders the perpetrator of the act or default liable to legal punishment". The concise Encyclopedia of Crime and Criminals,[8] has

[2] The New Encyclopedia Britannica, London: [1985] (5) *Encyclopedia Britannica*.
[3] McCabe, 'Crime' in D. Walsh and A. Poole (eds), *A Dictionary of Criminology*; (Routledge and Kegan Paul Publishers London. 1983), 49-52.
[4] G. Williams, 'The Definition of Crime: Current Legal Problems' [1955], 107.
[5] Tappan, P. Who is the Criminal? [1947] (12) *American Sociological Review*, 96—102.
[6] Gordon Stowell (ed), *Waverly Encyclopedia of Fact*: (Waverley Book Company. 1953).
[7] Halsbury Laws of England London (Butterworth 2016).
[8] H. Scott, 'Concise Encyclopedia of Crime and Criminals London' (Andre Deutsch Ltd. 1961), 84-85.

defined 'crime' thus: "A crime is an act or default which prejudices the interests of the community and is forbidden by law under pain of punishment. It is an offence against the State, as contrasted with loot or a civil wrong, which is a violation of a right of an individual and which does not lead to punishment". The Oxford Dictionary of Sociology[9] on its part defines crime in a more complex way: "an offence which goes beyond the personal and into the public sphere, breaking prohibitory rules or laws, to which legitimate punishments or sanctions are attached, and which requires the intervention of a public authority". While The Oxford English Dictionary[10] on the other hand, defines crime simply as: "An action or omission which constitutes an offence and is punishable by law".

The foregoing definitions of crime tend to focus on the act or omission being juxtaposed against the requirement of law. However, as several eminent criminologists recently have noted[11], the formula to understanding crime is to focus on fundamental attributes of all criminal behaviors rather than on specific criminal acts. Gottfredson and Hirschi[12] focused on criminality rather than crime and noted that criminality is a style of strategic behavior characterized by self-centeredness, indifference to the suffering and needs of others, and low self-control. "Acts of force or fraud undertaken in pursuit of self- interest". Consequently, they viewed almost all criminal acts as banal and trivial, need only short preparation, have little permanent consequences, and often do not produce the result that the offender had expected.

2.1.2. Concept of Cybercrime

The concept of cybercrime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and

[9] J Scott, 'Oxford Dictionary of Sociology' (3rd edn, Oxford University Press, 2005).
[10] S. B. Flexner, 2010 'Oxford English Dictionary' (3rd edn, Oxford University Press, 2010).
[11] For example, see Gottfredson, M. R., and Hirschi, T. '*A General Theory of Crime*' (Stanford University Press. 1990), 15.
[12] *Ibid*. 15.

counterpoised by the sanction of the state. Several authors have attempted to conceptualize what activity comes under the compass of cybercrime. Cybercrime denotes criminal activity including internet, computers or any other inter-connected infrastructure.[13] Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. Cybercrime has also been used to describe a wide range of offences, including offences against computer data and systems (such as hacking), computer- related forgery and fraud (such as phishing), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content).

Shinder[14] define cybercrime as any criminal offenses committed using the internet or another computer network as a component of the crime. Cybercrimes are offences that are committed against individual or group of individuals with a criminal motive to internationally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet and mobile phones.

McConnel[15] argued that cybercrimes differ from most terrestrial crimes in four ways, which are: They are easy to learn; they require few resources compare to the potential damage caused; they can be committed in a jurisdiction without being physically present and they are often not clearly illegal. As such, cybercrime has become one of the major security issues for law enforcement agencies and the world in general.

[13] Rajesh Kumar Goutam 'Importance of Cyber Security' [2015] (111) (7) *International Journal of Computer Applications*, 0975 — 8887.
[14] D. L. Shinder, 2002 'Scene of the Cyber-crime: Computer Forensics Handbook (Syngress Publishing Inc. USA 2022), 88.
[15]M. C. Connell 'Cybercrime and Punishment: Archaic Law Threaten' <www.iwar.org.ukresourcesmcconnell> Accessed 28th December 2023.

Maitanmi,[16] on his part considered cybercrime as being a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Cybercrime evolves from the wrong application or abuse of internet services.

According to the Council of Europe (COE) Convention on Cybercrime, cybercrime involves "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data"[17] Thomas and Loader conceptualize cybercrime as those "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".[18] Cybercrime may be said to be those species of crime where either the computer is an object or subject of the conduct constituting crime. That is to say, any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime.[19]

Flowing from all the above conceptualization of cybercrime, a common thread can he discovered which is the fact that all cybercrimes involve the use of computer with the computer either being used as a tool mediating the commission of the crime or being the end target of the crime. In some other cases both the computer and the person behind it may be victims of cybercrime.

---

[16] O. Maitanmi, S. Ogunlere and S. Ayinde 'Impact of Cyber Crimes on Nigerian Economy' [2013] (2) (4) *The International Journal of Engineering and Science (IJES),* 45—51.

[17] Council of Europe (COE). 2001 Convention on Cybercrime. <http://conventions.coe.Int/treaty/en/treaties/html/185/htm>. Accessed 28th December 2023.

[18] D. Thomas and B. Loader, 'Introduction to Cybercrime; Law Enforcement, Security and Surveillance in the Information Age' in D. Thomas and B. Loader (eds.), *Cybercrime: Law enforcement, Security and Surveillance in the Information Age* (Routledge London. 2000), 3.

[19] K. Dashora, 'Cyber Crime in the Society: Problems and Preventions' [2011] (3) (1) *Journal of Alternative Perspectives in the Social Sciences,* 240-259.

It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis and cybercrime is no exception[20]. Thus, even within the concept of cybercrime, there is sub classification depending on the main target of the crime whether it is the computer itself or the owner of the computer. Hence, the computer will be looked at as either a target or tool for simplicity's sake. The computer is considered as a tool mediating cybercrime when the individual is the main target of cybercrime. Cybercrime that come under this classification have previously been in existence in the offline and are merely facilitated by the use of a computer or internet connection. Such crimes generally target and exploit human weaknesses. The same criminal has simply been given a tool which increases his potential pool of victims and makes him more difficult to trace and apprehend. According to Dashora[21] these crimes generally involve less technical expertise as the damage done manifests itself in the real world. These crimes include for instance scams, theft, fraud, deception financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, cyber defamation, cyber stalking etc.[22] and they have existed even before the advent and development in the use of computers and internet networks.

The other sub classification of cybercrime involves those in which the computer is not merely a tool through which these crimes are committed but equally constitute the target of such crimes. Unlike crimes using the computer merely as a tool, these crimes require the technical knowledge of the perpetrators. These crimes are relatively new, having been in existence for only as long as computers have. Cybercrimes of this nature where the computer is the target rather than merely a tool are numerous and occur daily on the internet. Instances of such unlawful use of the computer include: unauthorized access to computer/computer system/

[20] O. S. Adesina, 'Cybercrime and Poverty in Nigeria' [2017] (13) (4) *Canadian Social Science*, 19-29.
[21] Dashora. (n19), 240-259.
[22] *Ibid.* 244.

computer networks, theft of information contained in the electronic form, e-mail bombing, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking etc. It is important to note that this classification of cybercrime into those wherein the computer is being used as a tool and others wherein the computer is being used as a target is not water proof. Instances abound where both areas overlap with one illegal cyber activity given result to the two circumstances. It is impossible to have a perfect airtight classification system.[23]

2.1.3. Concept of Cyber Security

The existence of crime always usually informs the corresponding adoption of means and methods towards its prevention and controlling the commission. This is true of all types of crime including cybercrime. Thus, the emergence of the internet that heralded cybercrime has necessitated the adoption of measure towards the prevention and control of cybercrime. These measures are collectively referred to as cyber security. Cyber security has thus been defined as technologies and processes constructed to protect computers, computer hardware, software, networks and data from unauthorized access, vulnerabilities supplied through internet by cyber criminals, terrorist groups and hackers[24]. The essence of cyber security then is to protect one's access to the internet and network based digital equipment and information from unauthorized access and alteration. Cyber security according to the UN International Telecommunication Union[25] is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications,

[23] *Ibid.* 240.
[24] K. G. Rajesh, 'Importance of Cyber Security' [2015] (111) (2) *International* Journal of Computer Applications, 0975—8887.
[25] United Nations International Telecommunication Union Cyber Security. <http://www.itu .int/en/ITU-T/studygrou ps/corn 17/Pages/cybersecurity.aspx>. Accessed 28th December 2023.

services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, integrity, which may include authenticity and non-repudiation and confidentiality

The United States of America National Initiative for Cyber-security Education (NICE): has equally advanced a definition of cyber security to mean the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation[26]

Furthermore, cyber security is considered to be a blanket term covering strategy, policy, and mechanisms regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure[27]. Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.[28]

Considering the fact that the present-day world is ruled by information and the relative importance of those information including national security information stored in the cyber

[26] Douwe Korff. 'Cyber Security Definitions: A Selection' <https://www.sbs.ox.ac.uk.>system >files>. Accessed 28th December 2023. Also available on <http://niccs.us-cert.gov./glossary#cybersecurity>.
[27] *Ibid.*
[28] University of Maryland, 'University College Introduction to Cyber Security' <www.umuc.edu.academic-programs/cyber-security?about.cfm>. Accessed 28th January 2024.

environment, and the extent of damages that can be caused if this information fall into wrong hands, cyber security should be the preoccupation of everyone exposed to the use of the internet whether directly or indirectly. Thus, the government, military, businesses, schools and indeed everyone that uses the internet has to ensure that sufficient precaution is taken to prevent unauthorized access to information stored in their computers. The increase in cybercrime and the evolving nature of the sophisticated means and methods through which it can be perpetrated further accentuates the need for cyber security to be an integral aspect in the use of the internet and forms an important part of the activities of individuals, organizations, businesses, government and educational institutions.

2.1.4. Concept of Internet

The internet is a worldwide, publicly accessible network of networks. The internet enables individuals and businesses to share information, resources, and services through interconnected computer networks. The internet can be employed in a variety of ways and for variety of purposes including for sending and receiving emails, web browsing, instant messaging, streaming music and videos, voice and video calls, online gaming etc.

Oyewole and Obeta,[29] state that the internet is the inter connection of computer across the world thereby creating unlimited opportunities for mankind. Internet has been viewed as a collection of networks and computers although the internet is designed for both communication capabilities and information services. Internet has further been characterized as "collectively the myriad of computer and telecommunications amenities, encompassing gear and functioning programs, which comprise the interconnected worldwide mesh of systems that provide work

[29] Oyewole and Obeta, 'An Introduction to Cyber Crime' (2002) <http://www.crirneresearch.org/articles/-crime>. Accessed 3rd February 2024.

the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to broadcast data of all types by cable or radio[30]

The US Federal Networking Council (FNC)[31] on the 24th of October 1995 unanimously passed a resolution defining the internet. Which definition of the "Internet" was developed in consultation with members of the Internet and Intellectual Property Rights Communities. Accordingly, the "Internet' refers to the global information system that:

i. is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons
ii. is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and
iii. provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein".

What is generally acceptable is the fact that the internet is and continues to evolve at a great pace. Internet traffic is growing, approximately doubling each year[32]. According to Ehimen and Bo1a[33], the internet has created a geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. The internet continues to revolutionize the way businesses are conducted as business transaction can be conducted between parties thousands of miles apart without the requirement of physical proximity.

[30] A. Yassir, and S. Nayak, 'Cybercrime: A Threat to Network Security' [2012] (12) (2) *International Journal of Computer Science and Network Security.*
[31] R. E. Kahn and V. O. Cerf 'What is the Internet (And What Makes It Work) Note XV' <https://www.cnri.reston.va.us/what_is_internet.html>. Accessed 3rd February 2024. Also available on <http://www.fnc.gov>.
[32] K. G. Coffman and A. M. Odlyzko, 'Growth of the Internet' <https://www.scienced I rect.com>. Accessed 3rd February 2024.
[33] O. R. Ehimen and A. Bola, 'Cybercrime in Nigeria' *Business Intelligence Journal* [2010] (3) (1).

2.1.5. Concept of Organized Crime

Organized crime is a most elusive and perplexing concept to define[34] According to Cowling, the fact that organized crime and criminal gangs by their nature are difficult to define, contributes to the absence of a universally acceptable definition.[35] Opolot points out that anyone who attempts to define the elusive concept of organized crime will be faced with a host of conceptual traps and obstacles. His conclusion is that many people, including researchers, police and the average person do not have an understanding of the nature, concept and the definition of organized crime.[36] There are multifarious ways of viewing the idea of organized crime. This multiplicity of approaches is informed by the fact that there are no one formulations that can contain within it the entire range of forms of organized criminality and take into account the economic, regional and ethnic differences that exist. There are thus two mainstream ways of through which the definition of organized crime can be approached: A structural model that is based on the view that an organized criminal group is the definitive element of organized crime and a crime model, which is based on the view that organized crime refers to an act or acts committed by either an individual or group. Obokata simply states that there are two main ways to understand organized crime which is either, a set of actors, or a set of activities.[37]

The UN Convention against Transnational Organized Crime (Palermo Convention)[38] rather than define organized crime defined organized criminal group. Article 2 of the international treaty offers the following definitions of "organized criminal group"

> a) "Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one Or

[34] A. J. Ianni Francis, and R. Ianni Elizabeth, The Crime Society: Organized Crime and Corruption in America New York (Meridian Book 1976),1.
[35] M. Cowling, Fighting Organized Crime: Comment on the Prevention of Organized Crime Bill 1998 (11 SACJ 350-374), 350.
[36] J. S. E. Opolot, Organized Crime in Africa, Jonesboro (Pilgrimage), 18.
[37] T. Obokata, Transnational Organized Crime in International Law Oxford (Hart Publishing 2010), 14.
[38] Adopted under UN General Assembly Resolution A/RES/55/25 on 15th November 2000 and entering into effect in 2003. As of May 2016, the Convention has 147 State Signatories and 186 State Parties.

more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

b) "Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.

Standing[39] subscribes to the notion that the definition of an organized criminal group is basically the same as that of organized crime. His contention implies that the definition of an organized criminal group by the Palermo Convention of 2000, is also the definition of organized crime. He further argued that the term illicit enterprise seems far more attractive than the muddled concept of organized crime.

Conklinh[40] approaching the definition of cybercrime from the angle of a set of activities rather than a set of actors stated that organized crime is a syndicated crime and is the violation of the laws on a large-scale basis by ongoing, tightly structured groups devoted to the pursuit of profit through criminal means.

Still considering organized crime from a crime model, Marion[41] on her part prefers the term crime venture to organized crime and defines it as a criminal activity carried out by a particular group of criminals on a regular basis. She cites examples of truck hijackings where members who have ties to syndicates, access skilled labour to carry out the job called outlets where they can get rid of stolen property.

Organized crime was also considered as a form of criminality characterized by a steady activity perpetuated by criminal organizations (organized groups and criminal associations) with a

[39] A. Standing, Rival Views of Organized Crime (Pretoria ISS), 66.
[40] J. E. Conklin, Criminology (9th edn, Pearson Boston 2007), 315.
[41] N. E. Marion, Government versus Organized Crime: New Jersey (Pearson Prentice Hall 2008), 5.

hierarchy structure, a material and financial base and connection to state structure, which exploit corruption mechanisms[42].

Doldovaya[43] has identified elements that define a criminal formation these include: the stability of a particular criminal formation, demonstrated by a prolonged nature of its activity, and the repeated accomplishment of similar criminal acts; distribution of roles between the members of the organization both along a vertical line and along a horizontal one; a hierarchical structure including, as a minimum, one person who leads the organization's activities; the concentration of efforts towards specific forms of criminal activity; intent to extract as much income as possible from criminal activity within the shortest time possible; presence of a system of mutual social aids for members of the group.

Williams and Savona[44] state that the term organized crime has long been a source of controversy and contention, probably because of the different ways in which various features of the problem are approached. They submit that experts are also concerned, however, with more controversial issues such as the size, structure and cohesion of criminal organizations. They conclude by saying that, on one end of the spectrum are those who see organized crime in terms of large hierarchical organizations that are structured rather like traditional corporations while, on the other end are those who contend that, for the most part, organized crime groups tend to be loosely structured, flexible and highly adaptable. They believe that, the real power and effectiveness of organized crime are found in these amorphous qualities. They

[42] N. Chitadze, 'Global Dimension of Organized Crime and Ways of Preventing Threats at the International Level' [2016] (15) (3) *Connection QJ*, 17-32. <https://doi.org/l0.11610/Connectjons.15.3.02>. Accessed 3rd February 2024.
[43] A. I. Doldovaya, *Criminology: University Textbook* (3rd edn. Moscow. Norma 2005), 510-511.
[44] P. Williams and E. U. Savona (eds) *The United Nations and Transnational organized Crime* London (Frank Cass), 3.

argue that, rather than resembling a formal corporate structure, organized crime more closely resembles a social exchange network in the community.[45]

2.2. Theoretical and Historical Foundations

Several theories have been formulated as regards the underlying factor behind why people engage in criminal activities despite the existence of penalties for such criminal engagement. These theories are multifarious and will be grouped under four broad predominant heads for the purposes of this research. The theories are: biological theory, the classical theory, the sociological theory and the psychological theory of crime.

2.2.1. Biological Theory of Crime

Biological theories of crime are grounded on the assumption that some people are born criminals and physiologically different from some others who are not criminals. As such the underlying factor why, people engage in criminal activities according to the proponents of this theory can be traced to an individual's genetic composition and has nothing to do with external influences. The main proponent of this theory is Cesare Lombroso.

Lombroso, a 19th Century Italian psychiatrist while expounding on the works of Charles Darwin came to a conclusion that criminals are atavistic in other word that they are 'evolutionary throwbacks' and as such, that their brain is mal-developed or not fully developed. These individuals are considered to reproduce in their person ferocious instincts of primitive humanity and inferior animals.[46] He further postulated that the absence of these physiological attributes can be recognized in outward appearance of criminals and distinct from the outward appearance of non-criminals. In his review of prisoners, he discovered that they shared a common physical attribute such as the shape of their head and scalp, size of ear and teeth,

[45] *Ibid*.4.
[46] Taylor Walton, and Young, *'New Criminology London'* (Routledge & Kegan Paul 1973), 41

sloping foreheads, large jaws and receding chin, lines on the palm etc. Thus, these identifiable features can help differentiate individuals with criminal inclination from another non-criminal.[47] On the whole, his theory posits that individual engagement in crime is a product of biology and biological characteristics inherent in criminals. His theory apparently has been faulted as physical features and attributes of individuals cannot be used to explain their inclination to criminal activities.

Beyond that of Lombroso, other biological theories have continued to develop albeit adopting a different approach. Thus, rather than measuring the physical features of the body, contemporary approaches focus on such things as: biochemical conditions for instance linked to hormonal imbalance or poor diet; Neuro-physiological conditions for instance learning disability caused by brain damage; genetic inheritance or abnormality.[48]

Another exponent of biological positivism is Professor Eysenck who postulated that underlying reason why people commit crime can be traced to the sensitivity of their autonomic nervous system. For him, criminals have a deficient autonomic nervous system, their reflexes are difficult to condition or extinguish easily.[49] This corresponds to his introversion/extroversion distinction, criminals being extroverts. His theory has been discredited as being based on an extraordinary and morally repugnant conception of human nature. For Taylor, 'men rob banks because they believe that they may enrich themselves not because something biological propels them through the door of a bank.[50]

However, whatever the approach may be, these theories trace the root cause of involvement in criminal activities within the individual and suggest that criminals are lacking in some

[47] Scottish Center for Crime and Justice Research: *Theories and Causes of Crime.* <http://www.sccjr.ac.uk/work-with-us/courses/Iearning-resources-for-schools/#what-is-crime >. Accessed 3rd February 2024.
[48] *Ibid.*
[49] H. J. Eysenck, 1964 Crime and Personality (Houghton Mifflin. Boston MA. 1964).
[50] Taylor Walton, and Young, *New Criminology* (Routledge & Kegan Paul. London), 61.

biological substances that non-criminals possess which propel them to engage in criminal activities.

2.2.2. Classical Theory of Crime

The Classical theory of crime credited to Cesare Beccaria postulates that human beings are essentially rational beings and as such capable of distinguishing and making a choice between right and wrong. Crime therefore according to the proponents of this theory is a product of human rational choice.[51] People engage in criminality because they want to and not because of any defect in their physiological composition. To curb the menace of crime, the classical theorist advocated for imposition of penalties severe enough to outweigh any form of pleasure derivable from the commission of criminal acts. These penalties will serve as a deterrent to check future engagement in criminality since humans being rational will willingly refrain from committing criminal acts once they had juxtaposed the pain with the gain and realized that the penalties attached to it would exceed the pleasure involved in the act itself. Several theories have emerged that expanded the classical theory such as the rational choice theory, the deterrence theory and the economic theory but these theories are in essence validating the stance of the classical theory that humans engage in criminal actions because they choose to and penalties which will serve as a deterrent is necessary to dissuade people from criminality. Severe punishment as suggested by proponents of this theory as a deterrent factor for curbing crime has however failed to produce the desired effect as people still engage in criminal activities despite the existence of severe punishment that outweighs the gain that is derivable from the crime even when the punishment is a death sentence.

[51] C. Beccaria, *Crimes and Punishments*, translated by H. Paolucci, (Bobbs-Merrill1. New York .963),

2.2.3. Psychological Theory of Crime

There seem to be an overlap between sociological theories and psychological theory of crime and delinquency. However, while the sociological theories address crimes and delinquencies at the macro level, looking primarily at the societal and environmental influences that lead to criminal behaviour. The psychological theories on the other hand address crimes and delinquencies at the micro (individual) level, focusing majorly on individual differences and peculiarities that lead to criminal behaviors.[52] The following theories will be discussed under the psychological theory of crime: the intelligence theory, personality traits theory, psychopath theory and cognitive and development theory.

i. Intelligence Theory

Intelligence theory postulates in essence that there is a connection between intelligence and delinquency. Goddard[53] for instance, when IQ became the measure of intelligence concluded that criminal behaviour was caused by low intelligence and as such majority of the inmates had low IQ. His theory therefore established a direct causal link between IQ and delinquency. However, subsequent research that try to establish a direct causal link between IQ and delinquency has been criticized for methodological reasons because as stated by Pfohl[54], there is wide variation between IQ scoring among criminals and non-criminals, good schooling can influence high IQ scoring, low motivation can lead to low IQ scoring etc.

Other research focus on the effect of IQ on delinquency among other factors to discover whether there is a direct causal link between IQ and delinquency or an indirect link mediated by other factors such as school performance[55]. Some studies have shown that intelligence has

[52] M. Moore, 'Psychological Theories of Crime and Delinquency' [2011] (21) *Journal of Human Behavior in the Social* Environment, 226—239.
[53] H. H. Goddard, *Feeble-mindedness* in D. 3. Shoemaker (ed.) *Theories of Delinquency: An Examination of Explanations of Delinquent Behavior* (Oxford University Press. New York 2005).
[54] S. Pfohl, *Imaged of Deviance and Social Control: A Sociological History* (McGraw Hill, New York. 1994), 113.
[55] J. M. McGloin and T. C. Pratt and J. Maahs, 'Rethinking the IQ-Delinquency Relationship: A Longitudinal Analysis of Multiple Theoretical Models' *Justice Quarterly* [2004] (21) (3), 603—635.

an effect on delinquency as delinquents were held to have lower IQ than non-delinquent[56]. However, this link is indirect and mediated by other factors for instance; the effect of IQ on delinquency as mediated by school performance. Thus, students with lower IQ scores did poorly in school, gained fewer acceptances, had fewer opportunities to excel at school and then, as a result, looked for acceptance and opportunities elsewhere[57]. The influence of school as a device of social control was therefore diminished for these students which consequently led to increased delinquent acts. Apart from school performance, other mediating factors in the indirect link between IQ and delinquency include deviant pressure groups and self-control[58]. Thus, under this intelligence theory, IQ has an indirect link with delinquency and impact some mediating factors such as school performance, influence of deviant pressure group and self-control and psychological wellbeing. It is therefore the impact that IQ has on these factors that indirectly leads to criminal activities and delinquency[59].

ii. Personality Traits Theory

The personality trait theory posits that criminal activities and delinquencies are both external manifestation of internal pathology. The prominent of this personality trait theory is that of psychoanalysis theory which was developed from the writing of Sigmund Freud. He posits that personality is developed early in life and is composed of three distinct parts: the id, the ego, and the superego. While the id represents the instinctual drives, the ego represents understood social norms that harness the id, and the superego is learned moral reasoning.[60] Hence, delinquency result from an imbalance between these three parts of our personality. The internal

[56] T. Hirschi and M. Hindelang, Intelligence and Delinquency: A Revisionist Review' *American Sociological Review* [1977] (42) (4), 571 —587.
[57] M. Moore, Psychological 'Theories of Crime and Delinquency' [2011] (21) *Journal of Human Behavior in the Social Environment* 226—239.
[58] *Ibid*. (n55), 503—635.
[59] *Ibid.* (n52), 226-239.
[60] L. J. Siegel and B. C. Welsh and J. J. Senna, *Juvenile Delinquency: Theory, Practice and Law* (Thomson and Wadsworth. Belmont. 2006).

conflict that leads to delinquency, usually between id and ego is seen as painful for the individual such that the individual pushes it to his subconscious and develops a coping strategy called defense mechanism to cope with the conflicts. These defense mechanisms can lead to problematic personality such as delinquency. In essence, delinquent behaviour is seen as the external manifestation of an internal disease.[61] This theory was expanded by Erikson who argued that delinquent behaviours are product of identity crisis created by internal turmoil.[62] This theory has been criticized for the inability to test identity crisis using empirical means. The utility of the theory is thus limited by the lack of evidence to support it and vast variability in human behaviour.[63]

iii. Psychopathology Theory

This theory is used to describe more serious and violent crimes. This theory exhibits similarity with the personality trait theory. The distinction between the two theories however lies in the fact that the focus of personality theory is on individual trait that conflict with each other while the focus of psychopathology theory is on a state of being that includes several distinct traits such that it comprises a disorder. As such psychopathology theorist consider serious and persistent crimes as an outward manifestation of mental illness and not just personality clash. Anti-social personality disorder, also called *psychopathy*, is the prominent disorder used in the explanation of criminal behavior from this viewpoint. *Psychopathy* was described as a "socially devastating personality disorder defined by a constellation of affective, interpersonal and behavioral characteristics, including a propensity to violate social and legal expectations and norms"[64]

[61] D. J. Shoemaker, *Theories of Delinquency: An Examination of Explanations of Delinquent Behavior* (Oxford University Press. New York. 2005).
[62] *Ibid.* (n60).
[63] *Ibid.*
[64] R. D. Hare, *Psychopathy: Affect and Behavior* in D. J. Cooke and A. E. Forth and R. D. Hare (eds), *Psychopathy: Theory, Research and Implications for Society Dordrecht, Netherlands* (Kluwer Academic Publishers1998).

iv. Cognitive and Social Development Theory

Cognition generally has to do with conscious mental activities and theorist in this field focus on mental processes that assists us in understanding our world and engaging in problem solving. Cognitive ability is developed in an individual through different stages of his life. These developmental stages are diversely classified. In relations to social development and delinquency, Moffitt[65] created two developmental patterns: adolescent limited and life-course persistent. According to him, increased rate of delinquency in adolescence shows that delinquency was a normative part of individual cognitive development which peaked in the teen and desisted. As such delinquency is a normal part of development which is later abandoned as one continues to develop. However, there are a number of delinquents that continue to offend into adulthood and develop a pathological personality[66]. Several risk factors that may contribute in life-course persistent type were identified to include: Neurological damage and difficult temperament in infancy, difficult parental temperament, environments that promote criminal values, problematic child and parent interactions, and inability to overcome obstacles that lead to decreased options for non-criminal success.[67] Thus, individual that engages in criminal activity picked up trait in the course of their development process and transmitted same from one stage of development to another due to these identified factors. This theory of a trajectory life course persistence for example problematic infancy leads to problematic childhood leads to problematic adolescence leads to adulthood criminal behavior has been refuted by research on adult offenders who began offending in adulthood and not as juveniles.[68]

---

[65] T. E. Moffitt, 'Adolescence-limited and Life-course-persistent Anti-Social Behavior: A Developmental Taxonomy' [1993] (100) (4) *Psychological Review*, 674—701.
[66] *Ibid.* 674-676.
[67] *Ibid*. 674.
[68] E. P. Eggleston and J. H. Laub, 'The Onset of Adult Offending: A Neglected Dimension of the Criminal Career' *Journal of Criminal Justice*, [2002] (30) (6), 603.

2.2.4. Sociological Theory of Crime

Given the inadequacies of biological theories in the explanation of causes of criminal behaviour, sociological theories were developed to explain underlying factors behind individual involvement in criminal activities. Sociological theories of crime focus on the societal and environmental influences that lead to criminal behaviour rather than, on biological or psychological composition of individual persons. Sociological theories were said to emerge in the early twentieth century[69] including the following theories:

i. Anomie

This theory was postulated by Durkheim in his classical work Suicide[70] where he contrary to the view that held sway at the time that crime was an abnormality caused by the individual difference between criminal and non-criminals posited that crime was normal in a society. He explained that human conduct and misconduct is not inherent in individuals but is a function of group and social organization. He attributed crime to strained social relation and social differentiation which is caused by division of labour. A simple society according to him is held together by a mechanical solidarity where works are monotonous marked by integration: a state of cohesion, strong social bonds, and the subordination of the self to a common cause. As division of labour intensifiers, the society becomes more complex and unified through organic solidarity based on interdependence among individuals. This weakening of the collective force of the society and extreme individualism according to him leads to deviant behaviour.[71]

ii. Chicago School Social Disorganization

This theory is attributed to sociologist at Chicago School who postulated that crime was a function of neighbourhood dynamics and not due to individual action. According to a study

[69] D. Zembroski, 'Sociological Theories of Crime and Delinquency' *Journal of Human Behavior in the Social Environment*, [2011] (21), 240—254.
[70] E. Durkheim, *Suicide.* (Free Press. Ney York 1951).
[71] *Ibid*, 209-214

conducted by them, they concluded that the causes of crime were entrenched in one area of the American society – the city slum and people became criminals by learning deviant cultural norms and values that hold sway within that society.[72] They viewed crime as a social problem in which the poor were driven by their environment into a life of crime due to criminal values replacing conventional ones and being transmitted from one generation to the next.[73] This breakdown of social control resulted in social disorganization.

iii. Cultural Transmission

This theory is an off shoot of the social disorganization theory of the Chicago School. Proponents of this theory have argued that the organization of a neigbourhood in a city was central to the prevention of delinquency by demonstrating how urban growth distributes people and crime spatially and how the crime rates differ among Chicago neighbourhoods.[74] Further, this theory postulates that the nature of a neighbourhood and the economic status and the culture values of the various neighbourhoods were crucial factors that influence in the commission of a crime and that ethnicity or the nature of an individual in a neighbourhood did not contribute to the likelihood of a crime. Disorganized neighbourhoods enabled the transmission of delinquent tradition from one generation to another in same way that language and other social norms are transmitted.[75] Cultural transmission theory in essence describe the existence of a coherent system of values supporting delinquent acts and where these socially learned behaviour are transmitted from one generation to the next.[76]

[72] J. F. Short Jr, 'Criminology: The Chicago School and Sociological Theory'
[2002] (37) (2) Journal of *Law and Social Change*, 107—115.
[73] *Ibid*. 173.
[74] C. R. Shaw and H. O. McKay, Juvenile Delinquency and Urban Area (University of Chicago Press 1972).
[75] *Ibid*. 174.
[76] *Ibid*. 173.

iv. Differential Association

This theory is an extension of the cultural transmission theory and was developed by Sutherland and Cressey[77]. This theory postulates that social groups were arranged differently. While some are organized in support of criminal activities, others are against it which refers to "differential social organization". Further, criminal behaviours are learned through social interactions wherein the opportunities that are favourable to the violation of the law differ from opportunities that are unfavourable to the violation of the law which refers to "differential association". A combination of these two theories constitutes a full explanation of crime. While differential association accounts for why an individual is drawn to crime, differential social organization accounts for why the spate of crime are more in some sectors of the society than others.

v. Strain Theory

The strain theory builds on macro-anomie. This theory explains that crime occurs as a result of the different ways that individual adapts or adjusts to achieve society set goals during anomie condition. According to Merton[78], anomie occurs when institutionalized norms are weaken due to the society placing an intense value on economic success. Individuals adjust or adapt to this anomie situation in five different ways and this offers an explanation as to individual involvement in crime. The first is conformity which is the acceptance of both cultural goals and institutionalized means. The second is "retreatisim" which is a deviant alternative where an individual rejects both the societal goals and means. The third is rebellion which is equally a deviant alternative where an individual not rejects societal goals and means but actively substitutes them with other goals and means. The fourth is ritualism which is where an individual respects the societal means even where the goals are not realistic. The last is

[77] E. H. Sutherland and D. R. Cressey, *Principles of Criminology* (Lippincott. Philadelphia1995).
[78] R. K. Merton, *Social Theory and Social Structure* (Free Press. New York. 1968), 194.

innovation which involves an individual accepting the goals and rejecting the means. Of all these methods of adaptations, innovation is said to be the common way of defining most criminal behaviour in that it occurs "when the individual has assimilated the cultural emphasis without equally internalizing the institutional norms governing ways and means for its attainment"[79]

vi. Delinquent subculture

This theory combines the postulations of differential association theory and the strain theory to explain deviant behaviours. Cohen[80] consolidated and expanded the two theories to explain how delinquent subculture arises. He explained that subcultures emerge primarily from city slum that are organized to support crime (differential association theory) among individuals who due to certain circumstances including those surrounding their birth could not meet the criteria of the respectable status system and thus embrace values that allow them to gain a status different from the mainstream status and afford them opportunity to reject respectable values that lies outside their reach (strain theory)[81]. Thus, these individuals reject both the middle-class goals and means of achieving them and substitute them with their goals and means which is developed into a subculture and passed from one generation to another as a result of continuous discontent with one's status and the lure of alternative forms of attainable goals and successes.[82]

vii. Conflict Theory

This theory was developed from the philosophies of Karl Marx[83]. Marx viewed crime as a symptom of social decline and the political state as a mechanism for the perpetuation of

[79] Ibid. 195.
[80] A. K. Cohen, Delinquent Boys: The Culture of the Gang (Free Press Glencoe 1955).
[81] *Ibid* p. 121
[82] *Ibid* p. 121, 133.
[83] K. Marx, *The Communist Manifesto* (International Publishers. New York. 1848, 1932)

capitalism, which was at the root of crime. Under this theory, crime is considered to be a product of conflicts over the distribution of resources and the illegitimacy of such a distribution, especially as it impacts the poor and the groups that seek to organize and bring conflict out into the open[84]. Another proponent of this theory Turk[85] claimed that crime does not result from the conflict arising from groups vying for power but rather was a result of some behavior defined as criminal being ascribed to the lower status groups by those with power and authority. For him, criminal status is defined by those with power (the 'authorities') and imposed on those without power (the 'subjects').[86]

2.3. Literature Review

As stated above, cybercrime is a phenomenon that is trending not just in Nigeria but also in most other countries of the world leaving in its trail negative effects. Attempts have been made and efforts concerted by learned authors to inquire into content and scope of cybercrime, its classification and typologies, the causes and consequences associated with the menace.

According to *Ehimen* and *Bola*,[87] the internet has in its wake, created a geometric growth and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by nations of the world. However, the internet is not associated in its entirety with advantages as it is susceptible to being abused and used as an instrument for the commission of crime.

[84] J. H. Turner and Marx and Simmel (rev edn), Reassessing the Foundations of Conflict Theory [1975] (53) (4), *Social Forces,* 618-627.
[85] A. K. Turk, *Criminality and Legal Order* (Rand McNally Chicago. 1969).
.[86] *Ibid.* 25, 45.
[87] O. R. Ehimen and A. Bola, 'Cybercrime in Nigeria' [2010] (3) (1) *Business Intelligence Journal.*

In the opinion of *Okeshola* and *Adeta,*[88] internet related revolution in information technology has brought about two edge functions. On the one hand, it has contributed positive values as with the proliferation of several businesses that can be conducted on the internet and on the other hand, it has produced a new wave of crime that threatens the order of the society. The duo considers cybercrime to be targeted at individuals or group of individuals with the motive of harming their reputation and causing both physical and mental harm while using the instrumentality of telecommunication networks. The extent of damages done by cybercrime is however far reaching and not limited to individuals and organizations but extends to national governments and as such may threaten national security and financial health of a nation.

According to *Kamini Dashora,*[89] crime has continued to be associated with man from time immemorial and the major antithesis to development. He observed that it is difficult to categorize crime into distinct groups as many crimes possess the inherent capacity to evolve on a daily basis such that one category of crime may evolve into another category.[90] Amongst the different categorization of crime, cybercrime is considered the latest and perhaps the most complicated problem in the cyber world. Cybercrime is then considered as a crime that is committed on the internet using the computer as either a tool or a targeted victim. Thus the computer may either be used to facilitate the commission of the crime in which case it is a tool or it may be the primary target of the crime. No matter what the case maybe, a computer is central to cybercrime.[91]

[88] F. B. Okeshola and A. K. Adeta, 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria' [2013] (3)(9) *American International Journal of Contemporary Research.*
[89] K. Dashora, 'Cyber Crime in the Society: Problems and Preventions' [2011] (3)(1) *Journal of Alternative Perspectives in the Social Sciences,* 240 – 259.
[90] *Ibid.* 240.
[91] *Ibid.* 241.

Dewanjee and *Vyas*[92] tried to make a distinction between cybercrime and computer crime. According to the duo, while cybercrime is basically associated with the use of internet and networks, computer crime may or may not be associated with internet or networks. This research submits that the view of *Dewanjee* and *Vyas*[93] is correct on the distinction between cybercrime and computer crime. It is submitted that computer crime pertains to criminal acts that are committed through the use of computer. Computer crime law prohibits a person from performing certain act without authorization, including; taking programs or data, introducing a virus or other contaminant into a computer system, using a computer in a scheme to defraud, interfering with someone else's computer access code or use etc. Meanwhile, cybercrime refers to online or internet-based illegal acts. Cybercrime and internet crime usually involves the use of computer and internet or cyber space. Cybercrimes remains strictly online. Computer crimes are crimes that affects a computer regardless of the involvement of a network, however, still there is a thin line between "computer crime" and "cybercrime". An example of cybercrime is phishing (you steal log in credentials from various people and use their accounts for malicious purpose). As can be seen with phishing, it only requires a browser and internet connection. In computer crime scenario, it does not necessarily need internet connection, it could be infecting a target with a virus through internet or accessing a neighbour's computer/laptop without consent. [94]

As regards the causes of cybercrime in the country, *Omodunbi* et al[95] identified unemployment as the major cause of cybercrime in Nigeria as over 20 million graduates are not gainfully

[92] R. Dewanjee and R. Vyas, 'Cyber Crime: Critical View' [2013] (6) (14) *International Journal of Science and Research (IJSR)* ISSN, 2319-7064,
[93] *Ibid.*
[94] The difference between computer crime and cybercrime <https://www.coursehero.com/file/p73g3ob/Difference-Between-Cybercrime-and-Computer-Crime-is-the-term-cybercrime-refers/>. Accessed 3rd February 2024.
[95] B. A. Omodunbi and others, 'Cybercrimes in Nigeria: Analysis, Detection and Prevention' [2016] (1) (1) *FUOYE Journal of Engineering and Technology*, 37.

employed and thus revert to the commission of crime including cybercrime for survival. Beyond unemployment, unhealthy quest for wealth which is fueled by greed, lack of strong legal framework proscribing cybercrime and weak security on personal computers were identified as further causes of cybercrime in the country.

Adesina[96] is of the strong view that there is a correlation between poverty and cybercrime such that the increase in the poverty level in the country despite the abundance of natural resources accounts for the alarming increase in cybercrime in Nigeria. Thus, any attempt at curbing the menace of cybercrime in the country has to start from eradicating poverty through development plans that will revitalize the economy and provide strategies for combating unemployment and poverty in the country. This research submits that poverty connotes a denial of choices and opportunities and constitutes a violation of human dignity. Poverty implies the lack of a basic capacity to participate effectively in society.[97] This study conceptualises poverty as a state of deprivation whereby access to basic institutions that ensure well-being are denied and individuals face increased susceptibility to indices of negative human development. Living in a state of poverty is characterized by inadequate access to food, healthcare, employment, and education. Poverty describes a state of perpetual vulnerability to the outbreak of communicable diseases, insecurity, violence, social exclusion, and crime. From this, we can see how pervasive poverty can trigger and escalate cybercrime in Nigeria. However, this research differs the opinion of *Adesina*,[98] that poverty is the sole cause of cybercrimes in Nigeria. With due respect to the author, causes such as; unemployment, ease of commission, low conviction rate of offenders, uncertainty of punishment, inadequate penal legislations, greed and laziness, peer pressure etc. are equally factors that account for the commission of cybercrimes in Nigeria.

[96] O. S. Adesina, 'Cybercrime and Poverty in Nigeria' [2017] (13) (4) *Canadian Social Science*, 19-29.
[97] Rawyat Deonandan, 'Defining poverty: A summary of competing models' [2019] (2) (1) *Journal of Social and Political Sciences*, 17–21.
[98] *Ibid.* (n87).

This research therefore seeks to address this gaps. Other causes as identified by *Maghu, Sehra* and *Bhardawaj*[99] include ease of access, negligence on the part of users of computers and the internet, revenge motive, poor law enforcement bodies which fail to deter the commission of the crime, desire for publicity or recognition. Urbanization involving a massive movement of people from the rural area to the urban area was further advanced by Hassan, Lass and *Makinde*[100] as one of the causes of increase incidences of cybercrime especially where there are no ready employment opportunities available for the migrants. Flamboyant lifestyle displayed by cybercriminals ranging from driving exotic cars, wasteful spending to wearing designer clothing, etc. culminating in wrong role modeling by the youth is further identified as some of the factors that influence young individuals to engage in this crime.

Wall[101] categorized cybercrime into four established legal categories to include: Cyber-trespass which entails crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses; Cyber-deceptions and thefts involving stealing (money, property), e.g. credit card fraud, intellectual property violations also referred to as piracy; Cyber-pornography comprising in breaching laws on obscenity and decency; Cyber-violence involving doing psychological harm to, or inciting physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking. This classification sub-divides cybercrime according to the object or target of the offence: the first two categories comprise "crimes against property", the third covers "crimes against morality", and the fourth relates to "crimes against the person".[102]

---

[99] S. Maghu and S. Sehra, and A. Bhàrdawaj, 'Inside of Cyber-Crimes and Information Security: Threats and Solutions' [2014] (4) (8) *International Journal of Information & Computation Technology*, 835-840.
[100] A. B. Hassan and F. D. Lass and J. Makinde 'Cybercrime in Nigeria: Causes, Effects and the Way Out' [2012] (2) (7) *ARPN Journal of Science and Technology*, 628. <http://www.ejournalofscience.org>. Accessed 3rd February 2024.
[101] D. Wall, 'Cybercrimes and the Internet' [2001] in D. Wall (ed.), *Crime and the internet* (Routledge. London), 3-7.
[102] O. S. Adesina, 'Cybercrime and Poverty in Nigeria' [2017] (13) (4) *Canadian Social Science*, 19-29.

Another categorization is that done by *McGuire* and *Dowling*[103] who drew a distinction between cyber-dependent crime and cyber- enabled crime. While the former is concerned with offences that can only be committed using a computer, computer network or other information and communication technology such as hacking, dissemination of viruses and other malicious software, the latter refer to traditional crimes which could be committed without the use of ICT but which are increased in their scale or reach by the use of computer such as fraud in the form of phishing e-mail, scam, online banking and e-commerce fraud; theft including identity theft, etc.

Similarly, *Maghu, Sehra* and *Bhardawaj*[104] classified cybercrime into computer assisted cybercrime and computer-oriented cybercrime. Computer assisted as the name suggests are those that make use of the instrumentality of computer for the commission of the crime such as data piracy, child pornography, internet time theft, online credit card fraud, illegal interception of materials. Computer oriented cybercrime unlike computer assisted cybercrime has the computer as target of the crime rather than an instrument through which the crime is committed. Computer oriented cybercrime includes hacking, forgery, altering website, cyber terrorism.

As to the typology of the crime prevalent in Nigeria, *Omodunbi et al*[105] identified several sectors with unique typologies of cybercrime in Nigeria. In the banking sector, they identified Bank Verification Number (BVN) Scams, Phishing, Theft of Bank Cards and Cyber-theft / Banking Fraud as the prevalent form of cybercrime in that sector. In e-commerce sector, they identified Software Piracy (Intellectual Property Theft), Sales Fraud & Forgery, Data and

[103] M. McGuire and S. Dowling, 'Cybercrime: A Review of the Evidence' [2013] Home Office Research Report, 75.
[104] S. Maghu and S. Sehra, and A. Bhardawaj, 'Inside of Cyber Crimes and Information Security: Threats and Solutions' *International Journal of Information & Computation Technology*, [2014] (4)(8), 836.
[105] B. A. Omodunbi and others, 'Cybercrimes in Nigeria: Analysis, Detection and Prevention' [2016] (1) (1) *FUOYE Journal of Engineering and Technology*, 38.

Airtime Time (DAT) theft from service providers. In the educational sector, Cyber-Plagiarism and Cyber-Pornography were listed as the prominent. In the social media sector, Nigerian-Prince (Beneficiary of a will) Scam, Charity Funds, Cyber-Stalking, harassment and Blackmailing Scam, Social-Hi-Jacking were identified as the prevalent.

The degree of the negative impact of cybercrime is untold. In respect of the economy, cybercrime has continued to have a worrisome effect on the nation's economy. According to a report by the Centre for Strategic and International Studies, UK published in 2014, it was estimated that the annual cost of cybercrime to Nigeria stood at about 0.08% of our GDP, representing about N127 billion.[106] Cybercrime also affect productivity rate. Cyber-attacks in the form of viruses and worms which have the capacity of slowing down systems, making servers inaccessible and jamming networks can adversely affect productivity and output generally which in turn affects the economy.[107]

Beyond the financial losses attributable to cybercrime, the scourge of the proliferation of cybercrime continues to bring the nation to disrepute in the international community. This has led to lack of trust and faith by foreigners involved in one business or the other with Nigerians. As reflected by *Ribadu*[108] "cybercrime is depressing trade and investment confidence in our economy and to that extent, it is a present and clear danger to our national security and the prosperity of our citizens". Furthermore, cybercrime has a negative impact on customer trust. This may occur where cybercriminals intrude into or clone a webpage, the end customers

[106] S. Iroegbu, 2016 Nigeria loses over N127bn annually through cybercrime. <http://www.thisdaylive.com/index.php/2016/04/19/Nigeria-loses-over-n127bn-annually-through-cybercrime/>. Accessed 29th December 2024.
[107] H. Saini and Y. O. Rao and T. C. Panda, 'Cyber-Crimes and their Impacts: A Review' [2012] (2) (2) *International Journal of Engineering Research and Applications* (IJERA) IS5N, 202-209. <www.ijera.com >. Accessed 29th December 2023.
[108] N. Ribadu, 2007. Cyber-Crime and commercial fraud: A Nigerian perspective. Presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL (United Nations Commission on International Trade Law), Vienna, Austria, 9-12 July. <http://www.cnudmi.org/pdf/english/congress/Ribadu_Ibrahim.pdf>. Accessed 29th December 2023.

visiting the page who becomes victim of a fraud may term the site fraudulent and this will discourage the use of the site in the long run.[109]

From the foregoing review of related literature, it is evident that most of the literatures concentrate on scope and content of the cybercrime within a particular national jurisdiction without reference to approaches employed in other jurisdiction in combating cybercrime. This research work builds on the threshold of these related literatures and finds utility in the fact that it makes a comparative analysis of the approaches and strategies adopted in other jurisdiction towards the prevention and control of cybercrime thereby drawing lessons to be gleaned by Nigeria in combating the menace.

This research submits that there is no single comprehensive explanation to account for the exhibition of deviant behaviour by individuals and human involvement in criminal activities. A lot of factors including biological, psychological and sociological factors may account for these factors and a combination of them may differ in their application to different individuals in different cultural background and at different dispensations.

2.4. Discussion on the Gaps

The various literatures reviewed in this study succinctly canvassed and notably majored on the causes and effects of cybercrime in Nigeria without addressing the combative measures through legal regime in the aftermath of commission of the offence i.e. arrest and investigation mechanisms, prosecution, conviction and certainty of punishment. Although no research can be exhaustive in solving a research problem, this research will attempt to address these gaps.

[109] H. Saini and Y. O. Rao and T. C. Panda, 'Cyber-Crimes and their Impacts: A Review' [2012] (2)(2) International Journal of Engineering Research and Applications (IJERA), ISSN, 206. <www.ijera.com>. Accessed 29th December 2023.

CHAPTER THREE
CYBERCRIME IN NIGERIA: TYPOLOGIES, CAUSES AND EFFECTS

3.1. Foundation to the History of Cybercrime in Nigeria

Africa's largest tech hubs, Nigeria, South Africa and Kenya were ranked in the top 100 for global cyber threats. This is according to a recent data report presented at the 2023 Golf Information Technology Exhibition (GITEX) event by Kaspersky Security Network (KSN). The report revealed that Nigeria currently ranked 50th worldwide for online threats and cyber-attacks vulnerabilities in Africa. South Africa ranked 82nd while Kenya found itself as one of the African countries with the most threats, ranking 31st.[1]

Cyber security has emerged as a critical concern for nations worldwide especially in the digitized world we live in today. Although, this is a worldwide challenge, developing countries such as Nigeria, South Africa, and Kenya, often find themselves particularly vulnerable to cyber threats, making them prime targets in the online threat landscape.[2] This could be as the security architectures in developing countries are not as robust as they are in other parts of the world. These cyber-attacks take different forms and are perpetrated through different methodologies employed by cybercriminals who are motivated by different motives. Several factors contribute to the existence and increase in the incidences of cybercrime in the country and these cybercrimes have different impact on individuals, organizations and the society in general. This chapter gives an insight on the classifications, typology, causes and effects of cybercrime in Nigeria.

[1] Kaspersky Security Network (KSN). <https://technext24.com/2023/06/07/nigeria-south-africa-kenya-cyber-threats/>. Accessed 28th January 2024.
[2] D. Otieno, 'Cyber security challenges: The Case of Developing Countries' [2020] <https://www.researchgate.net/publication/346485466_Cyber_security_challenges_The_Case_of_Developing_Countries>. Accessed 28th January 2024.

3.1.1. History of Cybercrime in Nigeria

The history of cybercrime in Nigeria is inextricably tied to the history of the internet in the country because cybercrime especially those that make use of internet connectivity emerged with the advent of the internet in Nigeria. The first ISP in Nigeria went live in the early 1990s, making the beginning of the modern internet age in the country. Before this, only persons who worked for the government or in academic institutions had access to the internet.

The National Center for Communication Technologies (NCCT) was founded in 1991 by the government of Nigeria, it was the country's first ISP (Internet Service Provider).[3] Afterwards, in the middle of the '90s, ISPs like; NITEL, Interswitch, and Vee Networks emerged to meet the need for private internet access. Corporations, governmental agencies, and educational institutions might use these service providers to establish internet connections. Unfortunately, the typical person was only presented with expensive and restricted alternatives. Access to the internet expanded rapidly in Nigeria beginning in the early 2000s.[4] Having a mobile phone in your pocket and the advent of new wireless technologies like GPRS and 3G have both played a role in this.

The growing number of Nigerians with access to the web has had a major effect on the country's culture and economy. This has resulted in an increase in people's ability to transmit and receive information and the development of e-commerce and internet-based enterprises. Nonetheless, Nigeria's internet has had its share of problems, including connectivity challenges, censorship, and security breaches. Both government and private

[3] Way back History of Internet in Nigeria. [2023]. <https://vtpass.com/blog/index.php/2023/05/02/wayback-history-of-internet-in-nigeria/#:~:text=The%20first%20ISP%20was%20founded,services%20to%20already%20burgeoning%20market>. Accessed 29th December 2023.

[4] E. E. Adom, Internet Development and Connectivity in Nigeria [2005] (39) (3) *Program electronic library and information system,* 257-268.

sector websites have been the subject of cyber-attacks, and periods of censorship of the internet have occurred.[5] Subsequently, in the year 2003, the first internet exchange point came into being in Nigeria and in the year 2005, the Nigeria Communications Commission got its own internet exchange point.

In 2009, the country achieved full local management of the country code domain name of 'ng.com' and since then the internet has continued to penetrate different sectors in the economy of the country.[6] With each passing year, the internet continues to experience different forms of evolution. However, with this evolution of the internet in the country come newer forms of cybercrime that continues to grow into a large and viable industry most patronized and dominated by the youth for different purposes due to different factors.

3.2. Classification of Cybercrime

Cybercrime has diversely been classified on the basis of subject (target) of the crime usually by considering the extent of the instrumentality of the computer in the commission of the crime[7]. In this regards, cybercrime has been classified into two categories: cybercrime with the computer as a tool and cybercrime with the computer as a target. Another form of classification of cybercrime is along the line of nature of the victim. In this regards, cybercrime has been classified into three categories: cybercrime against an individual, organizations and the society at large[8]. Furthermore, cybercrime has equally been classified according to the structural organization of the crime. Under this classification, there are two categories of cybercrime: cybercrime committed by an individual and organized cybercrime. Similarly, cybercrime has

[5] Detailed History of internet in Nigeria. < http://innovative.ng/detailed-history-of-internet-in-nigeria/>. Accessed 28th January 2024.
[6] *Ibid.*
[7] K. Dashora, 'Cyber Crime in the Society: Problems and Preventions' [2011] (3)(2) *Journal of Alternative Perspectives in the Social Sciences,* 240-259.
[8] *Ibid.* 248.

equally been classified along the line of the object of the crime[9] as distinguished from the subject of the crime. In this regards, cybercrime is classified into three categories: cybercrime against property, morality and the person. These classifications of cybercrime are however not cast in stone as there are overlaps within the classifications. One type of cybercrime may conveniently fit into more than one classification.

3.2.1. Classification by Subject

i. **Computer as a Tool:** The computer is considered as a tool mediating cybercrime when the individual is the main target of cybercrime. Cybercrime that come under this classification have previously been in existence in the offline and are merely facilitated by the use of a computer or internet connection. Such crimes generally target and exploit human weaknesses. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend. According to Dashora[10] these crimes generally involve less technical expertise as the damage done manifests itself in the real world. These crimes include for instance scams, theft, fraud, deception, financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, cyber defamation, cyber stalking etc.[11] and they have existed even before the advent and development in the use of computers and internet networks.

ii. **Computer as a Target:** the computer is not merely a tool through which these crimes are committed but equally constitute the target of such crimes. Unlike crimes using the computer merely as a tool, these crimes require the technical knowledge of the

[9] D. Wall, *Cybercrimes and the Internet* in D. Wall (ed.), *Crime and the Internet* (Routledge. London. 2001), 3-7.
[10] K. Dashora, 'Cyber Crime in the Society: Problems and Preventions' [2011] (3)(1) *Journal of Alternative Perspectives in the Social Sciences*, 240-259
[11] *Ibid*. 244

perpetrators. These crimes are relatively new, having been in existence for only as long as computers have. Cybercrimes of this nature where the computer is the target rather than merely a tool are numerous and occur daily on the internet. Instances of such unlawful use of the computer include: unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking etc.

3.2.2. Classification by Object

i. Cybercrime against Property:

This form of cybercrime just like the classification of cybercrime with the computer as a target directs it attack not to the person of the owner of the computer but rather to the property of such individual usually the computer. The form of cybercrime comprises mostly in cyber trespassing which involves crossing the boundary into another individual's property with the intention of causing damage.[12] The attack is not limited however to information stored or the computer hardware but extend to funds of the victim and also to intellectual property of such a person. Examples of this form of cybercrime include: hacking, defacement, transfer of viruses, credit card fraud, software piracy etc.

ii. Cybercrime against Morality:

This form of cybercrime rather than having the attack directed to the property of the victim has the attack directed against the sense of morality of the victim. Such cybercrime can be committed against an individual as well as the society at large. A typical example of such

[12] M. Olusola and others, 'Cyber Crimes and Cyber Laws in Nigeria' [2013] (2) (4) *The International Journal of Engineering and Science (IJES),* 19-25.

cybercrime is pornography including child pornography which is aimed at intentionally breaching the law on obscenity and decency as it is defined in a society.

iii. **Cybercrime against the Person:**

This form of cybercrime unlike the preceding two categories, targets the person of the victim and not just his properties or his sense of morality. This form of cybercrime is intended to cause psychological harm to the person of the victim and in some cases incites physical harm to be done to the person of the victim. Instances of this form of cybercrime include cyber stalking, defamation published over the internet, hate speech, cyber terrorism etc.[13]

3.2.3. Classification by Structural Organization

i. **Cybercrime by Individual:**

This sub classification of cybercrime focuses on cybercrime committed by an individual who is not a member of a syndicate and usually done as a one-off random act. Here, the perpetrator of this crime engages in such an offence as a sole venture and not in concert with other cybercriminals. Cybercrimes under this classification are not usually heavy as regards the intensity of the probable harm to result from its commission and the individual perpetrator may not have a career in crime but engages in the act as one-off act usually for the pleasure of such act rather than for financial benefits. Other factors that influence this form of cybercrime is peer pressure and sheer curiosity. Examples of such include: illegal streaming of video, music, illegal downloading of games etc. However, an individual may also pursue and undertake a career in cybercrime for financial gains and can equally commit crimes that are of an industrial scale like hacking and altering information on national security systems. The distinctive feature however is that the crime is committed by an individual who is not in criminal association with other persons.

[13] Dashora (n9), 20.

ii. **Organized Cybercrime:**

In contrast to cybercrime committed by an individual, organized cybercrime covers those committed by individuals working in concert with other criminals towards achieving a common goal. In this form of cybercrime, there is a structured organisation among the criminals involved, each having a designated role to play towards realising a common objective[14]. The underlying purpose is usually to derive financial gains that will be distributed amongst the conspirators however other purposes such as physical violence can influence such group such as in the case of cyber terrorism. Crimes of this category are usually large in magnitude and usually involve large sums of money. The distinctive feature of this form of cybercrime is the highly structured organization of two or more persons with a common target and division of roles.

3.2.4. Classification by Victimology

i. **Cybercrime against Individuals**

This classification focuses on victim of cybercrime. Under this sub-classification, individuals are the targets of this attack as opposed to organizations. It can be the person of the individual or his/her private properties. Cybercrime coming under this sub-classification include defamation, cyber-stalking, cybersquatting, fraud, indecent exposure, unauthorized access to system, transmitting viruses, computer vandalism, intellectual property theft, internet time theft etc.

ii. **Cybercrime against Organizations**

Rather than individual persons, organizations are the major target of theses cybercrime. Organizations such as companies, firms, NGOs, group of individuals as well as the government are usually the targets of these crimes although individual persons may ultimately be affected

[14] Dashora (n9), 19-20.

by these crimes[15]. Examples of these forms of cybercrime include: hacking into corporate websites, hijacking of websites and web pages, hijacking of corporate social media handles, unauthorized control/access over computer system, possession of unauthorized information, cyber terrorism against the government organization, distribution of pirated software etc.

iii. **Cybercrime against Society**

This form of cybercrime targets the society at large not just the constituents of the society. Such cyber-attacks may affect the general society including individuals and organizations in a society. These cybercrimes have a wider sphere of impact. Instances of such cybercrimes include online gambling, electronic trafficking, pornography including child pornography, indecent exposure, hate speeches etc.

3.3. Typologies of Cybercrime in Nigeria

Cybercrime is a blanket term used to refer to an avalanche of different crimes committed using the instrumentality of a computer and most times over internet connection. There are thus different types of criminal activities that come under the classification of cybercrime. However, there are those that are reoccurring and predominantly engaged in by cybercriminals in Nigeria. They include tile following:

a. **Yahoo Yahoo:** This is the most prevalent form of cybercrime in Nigeria. It is a variant of advanced fee fraud (419)[16] perpetuated over internet connection. It consists majorly of internet fraud with tile perpetrators referred locally as "yahoo boys or G-boys". It usually involves the use of scam email sent out by these yahoo boys to unsuspecting victims.[17] Various methods are employed to corner money

[15] *Ibid.* 20.
[16] Named after the provision of section 419 of the Nigeria Criminal Code Act (Cap C38) LFN, 2004 that created the offence of advanced fee fraud in the country and prescribes the punishment.
[17] O. S. Adesina, 'Cybercrime and Poverty in Nigeria' [2017] (13) (4) *Canadian Social Science*, 19-29.

from the recipients of these mails. For instance, these scammers may allege that they are entitled to huge sums of money left over to them by their deceased relative for which they require a little sum of money to process the requisite documents to get the money out. As such they will solicit the financial help of the recipient of the mail with a promise to refund the money given with additional lump sums. In other cases, they may allege that they are princes in a kingdom in Nigeria and require the recipient of the mail to send money over to them so that they can give one mineral resources or another to the recipient. Another reoccurring example is going to dating sites and hooking up with foreigners especially females who are seeking for a spouse. They pretend to fall in love with the foreigner and use that as a leverage to start exploiting the victim. They may demand money to process relevant travel documents to meet the victim and sometimes even get their victims to help in procuring travel documents to the victim's country of residence. Once these yahoo boys have achieved their aim, they break the communication link with the victim and move on to another victim.

The common trend is that these fraud stars play on the human weaknesses of their victim by appealing to their sense of pity and empathy. Another dimension to the yahoo-yahoo is what is now commonly referred to as YAHOO PLUS.[18] The difference between the aforementioned and yahoo-yahoo is the spiritual dimension. Perpetrators of the yahoo plus have been known to carry out fetish acts such as stealing women's underwear, eating excreta, taking peoples hair to make charms which they believe they will use to convince their victims to part with huge sums of money. These guys make occasional visit to their herbalist, pastors, alfas to get more

[18] T. Oludayo, 'A Spiritual Dimension to Cybercrime in Nigeria: The 'Yahoo Plus' Phenomenon'. 699. <https://www.researchgate.net/publication/272040780_A_spiritual_dimension_to_cybercrime_in_Nigeria_The_'yahoo_plus'_phenomenon> . Accessed 28th January 2024.

power so as to continue to make more money via the Internet. There is saying amongst these cybercriminals, that – "in Yahoo plus you don't rely on your brain alone. You need more than that". You need charm and other spiritual powers before conversing with your victims referred to as "maga".[19]

b. **Unauthorized access to computer systems or networks /Hacking:** Another form of cybercrime prevalent in Nigeria is hacking which involves gaining unauthorized access either physically or remotely to computer systems or networks with a motive to steal or destroy valuable information.[20] When these criminals gain access to the private information of the target, they may use same to commit other related offences such as illegal transfer of funds from the victims account to their account. These criminals employ different techniques and use different software that enables them to bypass firewalls and unlock pass words in order to gain access. Equally, they may crack security codes on e-commerce, e-marketing with a view to steal or destroy data. Although the usual motive behind the commission of this crime is to access private information to perpetuate other crimes, some hackers engage in hacking just for the fun of it or to gain respect from their fellow hackers or to build up reputation. Corporate organizations can equally employ hackers to retrieve valuable information from their competitors or to destroy valuable data.

c. **Software Piracy:** This typology of cybercrime is rampant in the entertainment industry. It involves in essence the unlawful reproduction of and sharing of application such as games, music and videos without the consent of the owner of the intellectual property. Cybercriminals make money from the illegal sales of pirated

[19] *Ibid.* 699.
[20] B. Omodunbi and others, 'Cybercrimes in Nigeria: Analysis, Detection and Prevention' [2016] (1) (1) *FUOYE Journal of Engineering and Technology*, 37-42. Also be accessed from <https://www.researchgate.net/publication/320411102_Cybercrimes_in_Nigeria_Analysis_Detection_and_Prevention> Accessed 28th January 2024.

copies of software. The internet has created a platform for almost anonymous, free and illegal distribution of pirated materials in Nigeria. Further social medias that support data sharing has also contributed to the menace of this type of cybercrime as the pirated software or illegally downloaded copy can easily be share amongst friends on social media.[21]

d. **Data and Airtime Time [DAT] Theft:** This form of cybercrime is prevalent amongst the youth and it is a form of hacking. Here the perpetrators illegally gain access to "Cheat codes" and unlawfully use them to gain thousands of mobile data and unlimited airtime without making the necessary payment.[22] Another variant of this type of cybercrime is internet time theft where the perpetrators illegally gain access to the connection of cyber cafes without paying any subscription fees and will be using such connection to browse free of charge. Cyber cafes on their own may be the perpetrators when they illegally connect to the network of internet service providers without paying any subscription fee.

e. **Cyber Pornography:** This is a type of cybercrime against public morality. It involves the recording and uploading of photography, films and videotapes with varying degree of sexual content on internet platform, especially materials depicting children engaging in sexual acts with adults[23] with a view of charging a fee from subscribers who view such phonographic items. Thus, beyond corrupting public morality, the perpetrators equally generate revenue from the commission of this offence. This typology of cybercrime is fast gaining grounds amongst the Nigerian

[21] *Ibid*. 37.
[22] *Ibid*. 39
[23] *Ibid*. 39

youth due to the fact that these pornographic articles can be accessed in the privacy of one's home with the use of a phone.[24]

f. **Social Media Account Hijacking:** This form of cybercrime involves hacking into the social media account of a user and hijacking same such that the perpetrator has access to utilize, make alteration and send messages from the account as though he is the owner. Social medial account hijacking has occurred in popular social media sites like Twitter, Facebook and Instagram. The hijacker once he is successful can post things and access things posted by the real owner of the account. Given that many people save sensitive information on their social media accounts such as their date of birth, residence and place of work, the criminal may be able to access personal information of the owner of the hijacked account with which other cybercrimes maybe perpetrated.[25] The criminal may demand for a ransom from the owner of the account in order to release the said account. Social media account hijacking can also be used to defame and tarnish the image of a victim since the hijacker can post any damaging thing on the personal page of the victim. These fraudsters also go as far as sending messages from the authorized page to friends and family requesting for money or any other kind of assistance[26]. Also, another common scenario also occurs when the fraudster creates a social page pretending to be someone else especially celebrities.

g. **Credit Card Theft or ATM Fraud:** Previously, the trend was to steal a bank card and compel the owner of the card to disclose the pin codes, thereafter, go to an ATM to withdraw funds from the account. Presently however, the theft of bank cards has

[24] *Ibid.* 39
[25] *Ibid*. 39
[26] *Ibid.* 40

evolved from the physical theft of the card to simply to the theft of the numbers.[27] Once the number on the card is stolen, the cybercriminal may be able to access remotely the funds in the account of the victim. Perpetrators of this crime adopt different methods in stealing the number on the credit cards of victims. For instance, credit card details from bank customers may be stolen when they type in the details in the internet pages of sellers of online transaction, when they pay using POS or when they are using the credit card information can then be used by the cybercriminal to purchase goods online to transfer funds in the account to other accounts.

h. Salami attacks: This kind of crime normally consists of a number of different smaller data security attacks which when pulled together end up resulting in one major attack. This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. This form of cybercrime is very common in banks where employees can steal small amount and it is very difficult to detect or trace.

i. Cyber Plagiarism: Plagiarism is the copying and use of another's work without referencing with a motive of passing off the work as one's original work. Cyber plagiarism is simply one done using internet connection or over the cyber. This form of cybercrime is prevalent in academic environment and it consists in essence the act of stealing peoples works, ideas or creations from the internet without acknowledgment of the source of the work and passing the work off as their original work.[28]

[27] *Ibid* p. 39
[28] See section 1(a) of the Copyrights Act, 2022 (Act No. 8).

j. **Cyber Stalking:** In simply term, cyber stalking means using the internet to stalk someone. As most people have their information online and on social media, the cybercriminal can easily access, this information and use it to stalk the target. This involves using the internet to repeatedly harass another. Stalking in the physical sense generally involves harassing or threatening behavior in which an individual engages repeatedly, such as following a person, appearing at a person's home or place of business, making harassing telephone calls, leaving written messages or objects, or vandalizing a person's property.[29] The nature of harassment may differ from victim to victim and includes sexual harassment, threat to life and property etc. The cybercriminal may follow the victims on an online platform or send unsolicited mails and obscene contents to the victim. It equally involves the sending of threat, defaming messages that may focus for example on gender, race, religion, nationality, sexual orientation etc. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties.

k. **Phishing:** This involves the cloning of a website or webpage of an e-commerce business in other to defraud unsuspecting customers who may not be able to differentiate between the original website and the cloned ones[30]. Cybercriminals can use this method to elicit personal information of victims including bank details and pass codes in other to gain unauthorized access to funds in their accounts. Phishing can equally involve sending an email to a victim that looks to the unsuspecting recipient as if it comes from a legitimate source, for instance, a bank. For example, an email is sent asking the victim to verify personal information through a link to a

[29] L. Ellison and Y. Akdeniz, 'Cyberstalking: The Regulation of Harassment on the Internet' [1998], *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet*, 29-48.
[30] M. Olusola 'Impact of Cyber Crimes on Nigerian Economy' [2013] (2) (4) *The International Journal of Engineering and Science* (IJES), 45-51.

fraudulent web page. Once that is provided, the hacker can access the victim's financial information. This type of cybercrime is prevalent in Nigeria especially in the banking sector. The year 2015 recorded high number of phishing emails from suspected cyber criminals in Nigeria, peaking when the Central Bank of Nigeria (CBN) announced deadline for Bank Verification Number (BVN). Cyber criminals swamped unwary bank customers with phish emails to warn them that their accounts were about to be blocked and consequently steal their credentials once they supply their details[31]

l. **Virus/Worm Attacks:** Viruses are computer programs that are intended to infect and destroy files with ability to replicate itself. The cybercriminal may send computer virus to the system of the target through diverse means such as through emails or link with intent to damage the software and hardware of the system of the target or to corrupt files and information stored on the computer. Malicious developers of anti-virus software sometimes intentionally create a computer virus and transmit it over the internet to millions of internet users and then develop an anti-virus that can remedy the effect of the virus. In this way, the developer will generate sufficient revenue from the sales of the anti-virus. Virus attacks can also be perpetrated by a competitor against another. Equally, discontented employees also engage in this crime by transmitting computer viruses to infect the files of their employer.

m. **Logic Bombs:** This is similar to virus attack but however differs in the sense that logic bombs do not replicate themselves unlike computer viruses. Logic bombs are essentially computer program that tells the computer to execute a set of instructions

[31] O. Richard, 'Nigeria: Putting the Cybercrime Law to Test in 2016' <http://allafrica.com/stories/201601060369.htmI>. Accessed on 17th January 2024.

at a certain date and time or under certain specified conditions.[32] These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. The instruction may involve the computer deleting all the information stored on it or resetting itself to default settings or totally crashing.

n. **Cyber Defamation:** Defamation is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium.[33] The fraudster sends e-mails containing defamatory content to people related to the victim or posts it on a website. This form of cybercrime is rampant on social media and practiced by people from different age brackets. The usual targets in this form of attack are mostly people in political offices and celebrities.[34]

o. **Cyber Terrorism:** According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents".[35] Unlike a nuisance virus or computer attack that result in a denial of service, a cyber-terrorist attack is designed to cause physical violence or extreme financial harm. According

[32] A. B. Hassan and F. D. Lass and J. Makinde, 'Cybercrime in Nigeria: Causes, Effects and the Way Out' [2012] (2) (7) *ARPN Journal of Science and Technology,* 628. < http://www.ejournalofscience.org> Accessed on 30th January 2024.
[33]A. C. Onuora and others, 'The Challenges of Cybercrime in Nigeria: An Overview' [2017] (1) (2) *AIPFU Journal of School of Sciences (AJSS),* 6-11. <https://www.researchga te.net/publication/338236273 The Challenges of Cybercrime in Nigeria An Overview>. Accessed 4th February 2024.
[34]*Ibid*.8.
[35] B. C. Collin, 'The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge' [1996] 11th *Annual International Symposium on Criminal Justice Issues.*

to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Apart from that, there is another dimension to cyber terrorism – the use of cyber infrastructure to launder money for financing physical terrorism. In 2005, FBI 50 officials reported that A1 Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases.[36] At least two views exist for defining the term cyber terrorism.[37] These are (1) Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals. (2) Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage. The terrorist's use of the internet and other telecommunications devices is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals.

p. Cyber Attack: Just as it is with the case of cybercrime, there is no universally accepted definition of cyber-attack. However, according to Hathaway,[38] 'cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose'. This definition pinpoints two basic peculiarities of cyber-attack. The objectives of a cyber-attack must be to undermine the function of a computer network, while also having a political or national security purpose.[39] A cyber-attack can include hacking, virus infection among others, but the

[36] J. K. Tudor, IS security Architecture, An Integrated Approach to Security in the Organization. (Auerbach Publications, USA 200).
[37] D. E. Denning, Information Warfare and Security. (ACM Press, USA1999).
[38] O. Hathaway and others 'The Law of Cyber-Attack' [2012] *Faculty Scholarship Series*; 817-885 at 833.
[39] *Ibid* p. 826-833.

objective can only be to undermine or disrupt the function of a computer.[40] However, computer crimes that are not carried out for a political or national security purpose, such as internet fraud, identity theft, and intellectual property piracy do not fit the requirements of a cyber-attack though they are cybercrimes.[41]

q. Cyber-Warfare: Cyber-warfare is substantially different from cybercrime as a whole, but unfortunately, computer networking technology has also blurred boundaries between cyber-warfare and cybercrime.[42] Cyber-warfare according to a scholar,[43] is a cyber-activity which consist of any action taken to undermine the functions of a computer network for a political or national security purpose, of which the effects must be equivalent to an "armed attack" or such activity must occur within the context of armed conflict. From this definition, it can be seen that cyber-warfare always meets the conditions of cyber-attacks. The element that differentiates it from cyber-attack is that the effect of the cyber-activity must also be equivalent to an 'armed attack' or the activity must occur within the context of an armed conflict. Cyber-warfare is also a distinct concept because cyber-warfare must also constitute a cyber-attack.[44]7

3.4. Causes of Cybercrime in Nigeria

Beyond the theories behind why people engage in criminal activities as examined in the preceding chapter which applies to crime and deviant behaviours generally, several factors

[40] *Ibid* p. 836.
[41] *Ibid* p. 830.
[42] Botnets, Cybercrime and Cyber terrorism: (2008) Vulnerabilities and Policy Issues for Congress Order Code <http://fas.org/sgp/crs/terror/RL32114.pdf>. Accessed 4th February 2024.
[43] *Ibid.* (n38), 833.
[44] *Ibid.* 88.

underlie the reason why individuals engage in cybercrime as a specie of crime in Nigeria. These causes far from being exhaustive and mutually exclusive to cybercrime include the following:

a. **Unemployment:** One of the major causes of cybercrime in Nigeria is unemployment and youth restiveness.[45] This is because most offenders are driven into this act due to lack of employment for graduates from secondary and tertiary institutions in Nigeria. It is a notorious fact that a significant number of Nigerian youths including graduates are not gainfully employed while others are under employed. This scourge of unemployment contributes in influencing these youths to engage in criminal activities in general and cybercrime in particular. Thus, unemployed youth can either resort to cybercrime as a means of self-employment or be lured into accepting employment by organizations that engage in cybercrime. Either way, cybercrime involvement is used as a means to escape the grasp of unemployment.

b. **Poverty/Financial Gains:** Poverty is another cause of cybercrime in Nigeria, where 40% of Nigerians live below the World Bank's threshold of less than US$1 per day.[46] World Bank Development report (2000) defines poverty "as an unacceptable deprivation in human wellbeing that can compromise both physiological and social deprivation". Poverty is the deprivation of basic resources that are necessary for maintaining the quality of life in terms of food, clothing, shelter and other rights and resources that can impinge on living conditions and guarantee human dignity.[47] The rate of poverty in Nigeria is alarming as such many cybercriminals engage in

[45] I. Umaru, 'The Impact of Cybercrime on the Nigerian Economy and Banking System'. [2019] (36) (12) *NDIC Quarterly.*
[46] Akintunde Akinleye/Reuters, 'Forty Percent of Nigerians live below the poverty line: Report' [2020] <https://www.aljazeera.com/economy/2020/5/4/forty-percent-of-nigerians-live-below-the-poverty-line-report >. Accessed 4th February 2024.
[47] B. Amaike, 'Quality of Life of Destitute Older People in Metropolitan Lagos, Lagos State Nigeria' [2011] (ix) *UNILAG Sociological Review (USR),* 6.

cybercrime out of desperation and in an attempt to survive. Given the perceived financial gains derivable from cybercrime, a lot of poor people engage in this criminal venture despite being aware that it is illegal and damning the consequences of their actions.

c. **Ease of Commission:** Some types of cybercrime are easy to commit requiring a minimum level of expertise to execute such crimes when compared to some other conventional forms of criminal acts. This makes it attractive to deviant individuals to engage in such criminal affairs. This ease is accentuated by the availability and accessibility of technology of cybercrime. Software tools can now be purchased online that allow internet user to locate open ports or overcome password protection. These tools allow a much wider range of people to become offenders, not just those with a special gift for computing. These tools can equally enable organized criminal groups to employ large numbers of relatively unskilled individuals to labour on their behalf.[48]

d. **Large Market:** The increase in the number of activities that can be executed with the aid of a computer has resulted in the increase in the number of computer and internet users which invariably mean increase in number of potential victims of cybercrime especially those of a financial nature. Increase in the number of internet users without a corresponding increase in the level of awareness amongst these users increase the risk and susceptibility to cybercrime thereby making the cybercrime industry a viable venture and a going concern.[49]

[48] M. McGuire and S. Dowling, 'Cyber Crime Investigation: Making a Safer Internet Space' *Research Report*, 75 <https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf>. Accessed 4th February 2024.
[49] A. Csuri, Cybercrime is World's Third–Largest Economy [2023] Threat Intelligence . Accessed 4th February 2024. <https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largest-economy>. Accessed 4th February 2024.

e. **Relatively Low Cost of Committing the Crime:** Cybercrime usually require low financial outlay to perpetrate when compared to some other conventional crimes. With as little as a cell phone or a laptop that has internet connection, one can easily commit crimes over the internet in different parts of the world. This factor is further prominent with the use of automation. A novice can thus exponentially increase the number of attacks by the use of automation. Many millions of unsolicited bulk spam messages can be sent out by automation within a short time frame and costing as little as nothing. Hacking can equally now be automated with millions of hacking activities going on at same moment reducing both tune and financial costs and making the venture more viable since at least one or two out of' millions of attempts may be successful.

f. **Hard to Detect:** Cybercrimes are usually hard to detect due to the fact that they can be committed remotely without the requirement of physical presence of the criminal. Thus from the comfort of one's sitting room, one can conveniently commit cybercrime in any part of the world. The sophisticated devices used by professional and advanced cybercriminals also reduce the chance of being detected by security outfits which most times cannot match the sophisticated devices and gadgets employed by these cybercriminals. Further, the use of automation helps these criminals to fly below the radar as they can get relatively low amount of money from relatively high number of individuals who may not bother to report the crime given the small amount of money involved.

g. **Revenge:** Cybercrime can also be committed out of revenge maybe by vengeful past employees who feel that they have been ill-treated. They therefore commit these offences as a way of getting back at their employer. These past employees can easily access the data base of their previous organization and commit these offences

due to the fact that they may have the pass codes which most organizations hardly change even after retrenching some of their staff. Furthermore, cybercrime can be committed by an organization against another with which they are in competition. In this regard, cybercrime is used as an instrument to perpetrate unhealthy competition. Instances of this cybercrime include hacking into an organization's system in order to compromise its information, viruses and worm attacks, logic bombs, email bombing etc.

h. **Low Conviction Rate:** Another motivating factor that influences people to engage in cybercrime is the low rate of conviction in respect of this class of offence. Conviction coupled with sentencing is usually used as instrument of deterrence to prospective criminals from engaging in a criminal conduct since a rational person will avoid a conduct once he sees the consequences of such. Thus, given the relatively low rate of conviction in respect of cybercrime which is caused by many factors such as difficulty in proving the commission of the offence as well as lack of adequate specialized training for prosecutors in this area of crime, people tend not to be deterred from engaging in cybercrime with the assumption that even if they are caught, they can easily get away without any criminal conviction.

i. **Dearth of Penal Legislations:** Absence of sufficient penal legislation in this field of crime equally contribute to the menace of the offence in our society. Some of the acts that pass as cybercrime have no substantive legislation proscribing such act and prescribing penalties for engagement in such act. As result, prosecutors cannot be able to charge perpetrators of these acts to court since a person cannot be charge for an act which does not constitute an offence at the time of its commission.[50] Inadequate legislation can also contribute to this menace where the penalties

[50] Section 36 of the Constitution of the Federal Republic of Nigeria 1999.

prescribed are not grave enough to deter prospective offenders from engaging or pursuing a career in cybercrime.

j. **Greed and Laziness:** Greed or get rich quick syndrome where youths want to jump the legitimate way of acquiring wealth which may take considerable time in favour of perceived quicker ways of acquiring wealth contribute in influencing people to engage in cybercrime of all sorts.[51] The desire to live above one's legitimate means, to live a luxurious and flamboyant lifestyle and show off equally drives individuals into cybercrimes.

k. **Societal Expectations:** The society tends to celebrate the rich and shun the poor. People who are wealthy receive respect and acknowledgment from the society without any consideration whatsoever of the source of their wealth. Thus people go out of their ways to engage in all sorts of inconceivable corrupt acts in order to acquire wealth with the assurance that there will be no form of stigmatization from the society as regards the source and means through which their wealth is amassed. These unreasonable societal expectation drive individuals especially the youths into cybercrime in an attempt to live up to the standards and expectations of the society.

l. **Distributive Justice:** Yet some cybercriminals engage in cybercrime out of their perceived sense of justice. These individuals believe that the rich and influential especially the politicians engage in corrupt practices, embezzle public funds and get away with it since they are seen as being above and the reach of the law, they therefore assume the responsibility of dispensing their own form of "justice" by targeting these perceived corrupt and rich politicians for their criminal activities.

[51] O. J. Nweke, 'The rapid growth of internet fraud in Nigeria, Cause, Effect and Solution' (2014) <https://innertempleoou.wordpress.com/2017/03/07/the-rapidgrowth-of-internet- fraud- in-nigeria-cause-effect-and-solution-by-nweke-oluchi-jacinta/ >, Accessed 4th February 2024.

These cybercriminals thus do not consider their actions as constituting an offence rather they believe that they are redistributing resources and dishing out justice to those that are beyond the reach of the law.

m. **Peer Pressure:** Pressure from deviant peer groups can equally cause an individual to engage in cybercrime. These individuals especially youths and adolescents in attempt to secure the approval of their peers and have a sense of belonging within their unit as well as to gain respect engage in one sort of cybercrime such as hacking, software piracy, illegal streaming of videos and music. Most others are persuaded; cajoled and even threatened into joining this deviant peer groups without their consent.

n. **Negative Role Model**: Another cause of cybercrime is negative role modeling. When criminals that engage in cybercrime are viewed by the youth as their role model, they will try to imitate the lifestyle of these criminals and may end up getting involved in cybercrime.

o. **Failure of the family system:** Some parents accept gifts above the means of their children without asking the source of the money spent on such gifts. A good number of them are aware of their children's involvement in internet fraud but rationalize it by claiming that it is a way of recovering our national wealth from our colonial masters.

3.5. Effect of Cybercrime in Nigeria

As noted by McAfee Inc[52] cybercrime is a growth industry, where the returns are great and the risks are low. They estimated the annual global losses from cybercrime to be more than 1 trillion USD. In the year 2023 it was estimated that Nigeria lost N1.27 billion annually to

[52] McAfee Inc. 2023 Net losses: Estimating the Global Cost of Cybercrime. <https://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf>. Accessed 4th February 2024.

cybercrime.[53] Cybercrime has become so widespread in Nigeria and the impact cannot be overemphasized as it affects both the rich and the poor in the society. The outbreak of COVID-19 pandemic and the lockdowns in the world further led to an increase in cybercrimes as most people had no option but to conduct their businesses and other activities via online which made the perpetrators to take advantage of the increased online transactions caused by the new normal.[54]

In the year 2017 and 2018 statistics has shown that Nigeria suffered an estimated annual loss of the sum of N250 billion and N288 billion respectively as a result of cybercrime,[55] which shows a significant rise of 54% from 2017 - 2018 growing at an average of 28,227 cybercrimes per month.[56] Some individuals in Nigeria have embraced cybercrime as a way of life. Many have become rich while some others have been caught by the law. This new crime is denting the image of Nigeria and drilling holes in the economy of the nation.[57] The negative impact of cybercrime is not limited to the financial loss of an individual or organization directly involved in the attack but goes far beyond that to include incidental negative impact to be felt by the society at large.[58] Some of the impact of cybercrime includes the following:

a. **Economic Impact:** Increase in dependence by most organizations and sectors of the economy on the internet to transact businesses lead to increased risk posed by cybercrime. Shares and stock are now traded online, bank transactions including

[53] G. Ewepu, 2016 Nigeria loses N127bn annually to cyber-crime — NSA available at: <http://www.vanguardngr.com/2016/04/Nigeria-losesn127bn-annually-cyber-crime-nsa/>. Accessed 4th February 2024.
[54] Andrey Popov, 'How COVID-19 Triggered the Digital and E-commerce Turning Point' <https://unctad.org/news/how-covid-19-triggered-digital-and-e-commerce-turning-point>. Accessed 4th February 2024,
[55] Security & Support Proshare 'Cybercrime in Nigeria', Causes and Effect' [2020]. <www.proshareng.com>. Accessed 8th February 2024.
[56] L. O. Donnell, 'Threat List: Nigerian Cybercrime Surged 54 percent in 2018' [2019] <threatpost.com/vulnerabilities>. Accessed 4th February 2024.
[57] O. Tade, and I. Aliyu, 'Social Organisation of Cybercrime among University Undergraduates in Nigeria' [2011] (5) *International Journal of Cyber Criminology*, 860–875.
[58] M. Olusola, 'Impact of Cyber Crimes on Nigerian Economy' [2013] (2) (4) *The International Journal of Engineering and Science (IJES)*, 45-51.

transfer of funds are done over internet connections, goods can equally now be bought online with the use of credit cards.[59] Cybercrime perpetrated against these established networks of business will have a direct impact on the individual, organization or firm involved and an indirect impact in the economy which will consequently be affected.[60] Cybercrime also discourage internet transaction especially with respect to previous victims of cybercrime who will be afraid and skeptical to carry out any transaction online. This impedes e-commerce and affects considerable amount of revenue that ought to be generated there from.

b. **Tarnishing the Reputation of the Country:** Nigeria has been classified amongst the top three countries in the world and the number one in Africa in cybercrime rating.[61] The exponential increase in the number of cybercriminals in the country committing different acts of cybercrime especially cyber fraud has made the country a hotspot for cybercrime and a dread to prospective investors.[62] The image of the country at the international community is dented and tarnished and discourages prospective investors from coming to invest in the country.

c. **Hinder International Trade:** Most aspects of international trade has gone digital with the effect that international trade between two parties that are countries apart can he consummated as a matter of minutes. Cybercrime especially cyber fraud and identity theft has the effect of instilling doubt and fear amongst international businesses parties who will be afraid of the genuineness of any transaction emanating from the country.

---

[59] Imhabekai Maryclaret Osi, *Prevention and Control of Cybercrime in Nigeria: Problems, Issues and Strategies* (A Dissertation submitted to the School of Postgraduate Studies, University of Ibadan, Zaria in Partial fulfillment for the award of Master of Laws (LLM), 2018).

[60] *Ibid.*

[61] D. O. Njoku, 'Ranking Countries with fear of Cybercrime in Africa' [2023] ResearchGate <https://www.researchgate.net/figure/Ranking-of-Countries-with-fear-of-Cybercrime-in-Africa-Source-World-Bank-Ease-of-Doing_fig1_338456129 >. Accessed 4th February 2024.

[62] Organised Crime in Nigeria: A Threat Assessment. [2023]. A research conducted by United Nations Office on Drug and Crime (UNODC). <https://www.unodc.org/ conig/uploads/documents /NOCTA_Web_Version _25.09.2023.pdf>. Accessed 4th February 2024.

This thus militates against the free flow of trade between local business men and their international counterparts.[63] This invariably affects the economy of Nigeria.

d. **Reduces Innovation:** When innovators and investors do not get returns from their inventions and investment due to cyber theft, they are discouraged from further research of innovative inventions and investment. Cybercrime such as software privacy, illegal streaming and downloading of videos and music deprive the copyright owners or originators of the intellectual properties from the benefits that accrue from same. This is a bane to creativity and innovation within our society.

e. **Consumers' Trust:** Cybercrime in the country equally has a negative effect on consumer and customers trust. Cyber-attacks such as denial of service attacks (DOS) has the effect of making consumers and customers of an internet related service to lose faith and confidence in such service-oriented organizations such as internet service providers, information and communication technology companies as well as, banks[64] etc. This in essence diminishes the number of customers or consumers that will patronize such an organization thereby leading to loss of revenue by such organization. Furthermore, consumers may equally be scared to transact businesses online like online shopping for fear of falling victim to cybercrime as the perception that the internet is rife with fraud continues to be on the increase. Hence, this concern over the insecurity of businesses conducted over the internet prevents many online shoppers from conducting businesses.

[63] E. F. G. Ajayi, **'**The Impact of Cybercrimes on Global Trade and Commerce [2016] (2)*' International Journal of Information Security and Cybercrime (IJISC),* 31-50. Also accessed on <https://www.ceeol.com/search/article-detail?id=517384>.

[64] M. Fan and O. Nunyuie, 'Investigating the Effects of Cyber Fraud on Customer Trust for Online Shopping: The Ghanaian Setting' [2019] (11) (39), 86-96. <https://core.ac.uk/download/pdf/276531331.pdf >. Accessed 4th February 2024.

f. **National Security:** the national security of most countries gradually is being dependent on internet connectivity and Nigeria is not an exception. Sensitive security information is passed from one security outfit to another. Any interruption with this information will have a grave repercussion as it can affect life and properties of Nigerians.[65] Terrorist groups in different parts of the worlds and in the country can equally use the internet connectivity to plan and execute their criminal activities. Funds can be transferred from one terrorist group in one parts of the world to another; international collaboration between different terrorist groups can be facilitated with the use of encrypted mails and messages. Although cyber terrorism in the form of a direct attack on government cyberspace and property is not yet prevalent in the country, however, with the increase in internet accessibility and accessibility of sophisticated devices, it is only a matter of time before terrorist groups if their activities are not checked will start to launch terrorist attack over the internet.[66]

g. **Facilitates other Crimes:** Cybercrime has the negative impact on the country in facilitating the ease of commission of other conventional offences. For instance, money laundering can most conveniently be committed with the use of internet connectivity. Murderer, kidnapper, rapist etc. can track down their victims online through cyber stalking without the victim even being aware that he/she is a target.[67] Burglary can be facilitated with alarm systems being remotely disabled and electric locks being remotely compromised. Trafficking of persons and illicit goods such as hard drugs can

63. R. Benfield and A. Dockar 'Cyber-attack: Is your Property Adequately Protected' [2018]. <https://hsfnotes.com/realestatedevelopment/2018/05/17/cyber-security-is-your-property-adequately-protected/>. Accessed 4th February 2024.

64. G. Weimann, Cyber 'Terrorism: How Real is the Threat?' [2014] Unite States Institute of Peace. *Special Report 119.* <https://www.usip.org/sites/default/files/sr119.pdf>. Accessed 4th February 2024.

[67] L. J. Stalans and M. A. Finn 'Understanding How the Internet Facilitates Crime and Deviance' [2016] (11) (4). *An International Journal of Evidenced-based Research, Policy, and Practice.* Accessed 4th February 2024. <https://www.tandfonline.com/doi/full/10.1080/15564886.2016.1211404>.

also be facilitated over internet connections. Private information of individuals can be unlawfully accessed and used to blackmail them.[68]

In concluding this chapter, this research submits that, there are different classifications of cybercrime but that notwithstanding, they all share a common denominator of having a computer and most times internet connectivity being used and abused in the commission of criminal activities. Amongst these classifications, cybercrime manifest itself in varied types with some prevalent in Nigeria and mostly subscribed to by cybercriminals in Nigeria including yaoo-yahoo, credit card fraud, hacking, software piracy, social media account hijacking, cyber plagiarism etc. The scourge of cybercrime together with the growing incidence of same is caused by an interplay of several factors prominent amongst which is the high incidence of poverty in the country as well as unemployment rate especially amongst graduate youths. These two predominant factors continue to contribute to the exponential growth of the cybercrime industry in Nigeria which leaves in its trail a plethora of negative impacts that go beyond the financial losses of individuals and organizations directly involved as victims of the menace of cybercrime to affect the society as a whole.

[68] *Ibid.*

CHAPTER FOUR
LEGAL AND INSTITUTIONAL FRAMEWORKS FOR CONTROL AND PREVENTION OF CYBERCRIME IN NIGERIA

4.1. Legal Foundation for the Prevention and Control of Cybercrime in Nigeria

The domains of modern activities have extended beyond the turfs of land, sea, air and space to include the cyberspace, where criminal activities have progressed almost unhindered. Organised crime groups and cyber criminals are working together seamlessly, moving between the real world and virtual environments.[1, 2] There are however various mechanisms for combating the menace of cybercrime in the country. The starting point is having the appropriate substantive legislation in place first to criminalize and provide punishments for several acts that constitute cybercrime, then to provide for procedure for the investigation, collection and collation of evidence and prosecution of suspected offenders in the court of law. This chapter is tasked with reviewing the normative legislations in force in Nigeria that have bearing on cybercrime in one way or another and the regulatory agencies responsible for monitoring, preventing and investigating cybercrime in Nigeria. Further the challenges that bedevil the investigation, prevention and control of cybercrime is considered and finally, approaches adopted in other jurisdiction is considered towards proffering lessons to be garnered by Nigeria in its fight against cybercrime.

Several extant legislations in Nigeria contain provisions dealing with one aspect of computer enabled or computer dependent crime as well as prescribing different penalties for commission of such offences. Although the provisions that have bearing on cybercrime contained in these legislations are inchmeal. In a bid to collate the scattered fragments of legislation and also to

[1] The fight against Transnational Cyber Crime in April 2007, the Strategic Alliance Cyber Crime Working Group (SACCWG) released its white Paper Transnational Cyber Crime and agreed that Combating Cyber Crime requires Transnational leadership and Cooperation. Platypus Magazine (96th edn, September 2007), 6-36.

[2] Nigerian Cybercrime Ring's Phishing Tactics Exposed. Infosecurity Magazine (May 2023). See also <https://www.infosecurity-magazine.com>. Accessed 27th February 2024.

make comprehensive provisions on cybercrime, the country enacted in 2015 a legislation that dealt exclusively and comprehensively on cybercrime. The following include legislations that have bearing on cybercrime in Nigeria.

4.2. Domestic Legal Framework for the Prevention and Control of Cybercrime in Nigeria

4.2.1. The Nigeria Criminal Code Act 2004:

The Nigerian Criminal Code Act[3] is the general law defining criminal offences and prescribing punishments for the commission of those offences in form of imprisonment and fines. The Criminal Code does not contain any direct or explicit provision mentioning cybercrime but however, there are provisions that cover cybercrime in the law. The two most prominent being section 383 and section 419 of the Act.[4]

Section 383(1) of the Criminal Code defined the offence of stealing and prescribed the punishment for the said offence. The said section provides thus:

> Any person who fraudulently takes anything capable of being stolen, or fraudulently converts to his own use or to the use of any other person anything capable of being stolen, is said to steal that thing.

The definition of the offence of stealing as defined in the above section covers stealing in whatever form and in whatever manner it is being committed so long as the item allegedly stolen is something capable of being stolen. Thus, cybercrimes that involves stealing whether of funds, data, information and whether or not the stealing was physically performed or was carried out through electronic means can conveniently come under the definition of stealing and the perpetrator can be tried and if found guilty convicted under the provisions of this Act.

[3] CCA Cap C38 LFN 2004.
[4] *Ibid.*

Another section of the Criminal Code that has a close bearing to cybercrime is sections 418 and 419 of the Criminal Code Act.[5] Both sections deal with advanced fee fraud. While section 418 defines the offence, section 419 contained the punishment for the offence. Section 418 provides thus:

> Any representation made by words, writing, or conduct, of a matter of fact, either past or present, which representation is false in fact, and which the person making it knows to be false or does not believe to be true, is a false pretence.

While section 419 states thus:

> Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

The above provisions of the code have a direct application to cybercrime although the word cybercrime is not explicitly contained in them. This is so considering the fact that most forms of cybercrime especially those prevalent in Nigeria involves one form of deception or false pretense or the other. For instance, 'yahoo-yahoo' which is the most prevalent cybercrime in Nigeria where 'yahoo boys' send fraudulent mails to unsuspecting individual mostly foreigners in order to obtain money from them is essentially obtaining by false pretense save that the representation and the obtaining are virtually done over internet connection.

A close examination of the provisions will show that there is no restriction as to the manner through which a false representation will be made in order to constitute an offence. Section 418 states that the representation can be in any form: "Any representation made by words, writing, or conduct". As such, whether the false representation is conveyed through physical

[5] *Ibid.*

communication by spoken words or conveyed through virtual communication or communication over internet connection by mail, messages, social media chats etc., so long as the representation is false to the knowledge of the maker or the maker does not believe in the truth of the representation and obtains on the basis of the representation anything capable of being stolen with intent to defraud, the maker is guilty of the offence of obtaining by false pretense and can be so tried and convicted under this provision.

4.2.2. The Economic and Financial Crime Commission Act, 2004

The Economic and Financial Crime Commission Act[6] (hereinafter referred to as the EFCC Act) provides for the establishment of the Economic and Financial Crime Commission and created some financial offences. Like the Criminal Code Act, the EFCC Act did not explicitly mention cybercrime in its provisions but however, the Act while prescribing the duties of the Commission and while defining some economic and financial offences shows that it has direct application to cybercrime especially those of a financial nature.

By Section 7(2) of the EFCC Act,[7] the Commission is charged with the responsibility of enforcing the provisions of laws relating to economic and financial crimes, including:

i. The Money Laundering (Amendment) Act 2004 and 2011.
ii. The Advance Fee Fraud and Other Fraud Related Offences Act 2006
iii. The Corrupt Practices and Other Related Offences Act 2000 (ICPC Act 2000).
iv. The Failed Banks (Recovery of Debts) and Financial Malpractices Banks Act 1994.
v. The Banks and other Financial Institutions Act 1991; and
vi. Miscellaneous Offences Act, 1985,
vii. Terrorism (Prevention) Act, 2011 and 2013 (2022 as amended) and
viii. Any other law relating to economic and financial crimes including the criminal code and the penal code.

[6] EFCC (Establishment) Act 2004.
[7] *Ibid.*

Section 46 of the Act[8] which is the definition section defined "economic and financial crimes" to mean:

> The non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited goods, etc.

From the above definition of economic and financial crimes, it is clear that cybercrimes of financial nature such as credit card fraud, ATM card theft, unauthorized hacking with motive to transfer funds. Yahoo-yahoo, software piracy etc. are within the contemplation of this Act. Offenders can thus be conveniently charged to the court and prosecuted under the provisions of this Act.

Further, section 6 of the EFCC Act[9] provides the functions of the commission to include inter alia the following:

The Commission shall be responsible for -

(a) the enforcement and the due administration of the provisions of this Act;[10]
(b) the investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc.;
(c) the co-ordination and enforcement of all economic and financial crimes laws and enforcement functions conferred on any other person or authority;

[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*

(d) the adoption of measures to identify, trace, freeze, confiscate or seize proceeds derived from terrorist activities, economic and financial crimes related offences or the properties the value of which corresponds to such proceeds;

(e) the adoption of measures to eradicate the commission of economic and financial crimes;

(f) the adoption of measures which includes coordinated preventive and regulatory actions, introduction and maintenance of investigative and control techniques on the prevention of economic and financial related crimes;

(g) the facilitation of rapid exchange of scientific and technical information and the conduct of joint operations geared towards the eradication of economic and financial crimes;

(h) the examination and investigation of all reported cases of economic and financial crimes with a view to identifying individuals, corporate bodies or groups involved;

(i) the determination of the extent of financial loss and such other losses by government, private individuals or organizations;

(j) collaborating with government bodies both within and outside Nigeria carrying on functions wholly or in part analogous with those of the Commission concerning –

i. the identification, determination, of the whereabouts and activities of persons suspected of being involved in economic and financial crimes,
ii. the movement of proceeds or properties derived from the commission of economic and financial and other related crimes;
iii. the exchange of personnel or other experts,
iv. the establishment and maintenance of a system for monitoring international economic and financial crimes in order to identify suspicious transactions and persons involved,
v. maintaining data, statistics, records and reports on person, organizations, proceeds, properties, documents or other items or assets involved in economic and financial crimes;
vi. undertaking research and similar works with a view to determining the manifestation, extent, magnitude, and effects of economic and financial crimes and advising government on appropriate intervention measures for combating same.

(k) dealing with matters connected with the extradition, deportation and mutual legal or other assistance between Nigeria and any other country involving Economic and Financial Crimes;

(l) The collection of all reports relating suspicious financial transactions, analyse and disseminate to all relevant Government agencies;

(m) taking charge of, supervising, controlling, coordinating all the responsibilities, functions and activities relating to the current investigation and prosecution of all offenses connected with or relating to economic and financial crimes;

(n) the coordination of all existing economic and financial crimes, investigating units in Nigeria;

(o) maintaining a liaison with office of the Attorney-General of the Federation, the Nigerian Customs Service, the Immigration and Prison Service Board, the Central Bank of Nigeria, the Nigeria Deposit Insurance Corporation, the National Drug Law Enforcement Agency, all government security and law enforcement agencies and such other financial supervisory institutions in the eradication of economic and financial crimes;

(p) carrying out and sustaining rigorous public and enlightenment campaign against economic and financial crimes within and outside Nigeria and;

(q) carrying out such other activities as are necessary or expedient for the full discharge of all or any of the functions conferred on it under this Act.[11]

From these functions of the Commission as conferred on them by the EFCC Act,[12] it is obvious that the Commission can investigate cases of cybercrimes especially those that are of economic and financial nature. The function of the Commission as stated above covers investigation of financial crimes including advanced fraud. Illegal charge transfer, fraudulent encashment of negotiable instrument, computer credit card fraud, contract scam etc. All these are instances and examples of cybercrime committed in Nigeria. The EFCC Act thus, has its application extended to cybercrime in Nigeria and cybercriminals can be prosecuted under the Act.[13]

In similar vein, section 7 of the EFCC Act[14] provides for the special powers of the Commission to include:

[11] EFCC Act (n6).
[12] *Ibid*.
[13] *Ibid* s13(2)
[14] *Ibid.*

> The power to cause investigation to be conducted into the properties of any person if it appears to the Commission that the person's lifestyle and extent of the properties are not justified by his source of income.

This provision of the Act further empowers the Commission to investigate the activities of cybercriminals as most of them usually always tend to live beyond their means. They are notorious for driving flashy cars, spending extravagantly, wearing designer clothes, living in expensive houses all of which their legitimate income cannot afford. On the basis of this section 7 of the EFCC Act which does not restrict the investigation to government officials, the Commission can investigate cybercriminal as well and prosecute offences under the EFCC Act.

4.2.3. Advance Fee Fraud and other Fraud Related Offences Act 2006

The Advanced Fee Fraud and other Fraud Related Offences Act[15] (hereinafter referred to as the Advance Fee Fraud Act) was enacted as an Act to prohibit and punish certain offences pertaining to advanced fee fraud and other fraud related offences. The Advance Fee Fraud Act although it contains related provisions as regards dealing with electronic telecommunication offences, it does not deal with the broad spectrum of computer abuse and cybercrimes. However, just like the EFCC Act, despite the fact that it has no explicit provision that makes mention of cybercrime, certain provisions of the Advance Fee Fraud Act have application to cybercrimes.

Section 1 of the Advance Fee Fraud Act[16] defined the offence of obtaining by false pretense thus:

> 1(1) notwithstanding anything contained in any other enactment or law, any person who by false pretense and with intent to defraud;
> a) obtains from any other person in Nigeria or in any other country for himself or any other person; or
> b) induces any other person in Nigeria or in any other country, to deliver to any person; or

[15] AFFFRO Act 2006.
[16] *Ibid*. s1(1)(2)(3).

c) obtains any property, whether or not the property was obtained or its delivery is induced through the medium of a contract induced by false pretense commits an offence under this Act.

1(2) A person who by false pretense and with the intent to defraud induced any other person in Nigeria or in any other country, to confer a benefit to him or on any other person by the doing or permitting a thing to be done on the understanding that the benefit has been or will be paid for commits an offence under this Act.[17]

1(3) A person who commits an offence under subsection (1) or (2) of this section is liable on conviction to imprisonment for a term of not more than 20 years and not less than seven years without the option of a fine.[18]

Section 20 of the Advance Fee Fraud Act[19] which is the general definition section of the Act defined false pretense thus:

> False pretence means a representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true.

The above provisions are without doubt applicable in some respect to cybercrime where the cybercriminal makes a false representation to another with intent to defraud. The Advance Fee Fraud Act is more elaborate in that it extended the geographical scope of the representation to go beyond the shores of Nigeria. Thus, even where the representation is made to someone that is outside Nigeria which in most case is what these cybercriminals do, the offense of obtaining by false pretense will still have been committed.

The Advance Fee Fraud Act also in sections 12 and 13[20] provides for duties of internet cafes and telecommunication companies. It provides that any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form shall

[17] *Ibid.*
[18] *Ibid.*
[19] *Ibid.*
[20] *Ibid.*

obtain from the customer or subscribers their full names, residential address, in the case of an individual, corporate addresses, in case of corporate bodies.

This provision which was enacted in a bid to monitor activities of internet users in order to prevent cybercrime seems not to be effective since people can access the internet from the comfort of their homes remotely and need not go to cyber cafes.

4.2.4. Child's Rights, Act 2003

The Child's Rights Act[21] (hereinafter referred to as the CRA) is the domestic legislation that domesticated the provisions of the Convention for the Rights of a Child and the African Charter on the Rights and Welfare of a Child.[22] The CRA[23] makes provisions for the protection of the rights and welfare of the Nigerian child. The CRA however has an indirect link to an aspect of cybercrime which is child pornography and prohibition of importation of harmful publication.[24] Section 30 (1) of the CRA[25] provides that no person shall buy, sell, hire, let on hire, dispose of or obtain possession of or otherwise deal in a child. Subsection 2(e) however provides that a child shall not be procured or offered for prostitution or for the production of pornography or for any pornographic performance.[26] Subsection 3 of section 30 criminalized the act and prescribed the punishment for the offence to be imprisonment for a term of ten years. The subsection provides thus: A person who contravenes the provisions of subsection (1) of this section commits an offence and is liable on conviction to imprisonment for a term of ten years.[27]

[21] CRA 2003 (Act No. 26).
[22] Articles 1 and 2. African Charter on the Rights and Welfare of the Child. Adopted by the 26th Ordinary Session of the Assembly of Heads of State and Government of the Organization of Africa Unity (OAU) in Addis Ababa, Ethiopia - July 1990 Entered into force on 29th November 1999.
[23] CRA s1(n21).
[24] CRA s35.
[25] *Ibid.*
[26] *Ibid* s30 (2)(e).
[27] *Ibid* s30 (3).

This provisions of the CRA equally touches on cybercrime considering the fact that child pornography is a form of cybercrime that continues to gain grounds in the country. Thus offenders can conveniently be charged and prosecuted for the cyber offence of child pornography under this provision of the CRA[28] and if found guilty punished in accordance with the dictates of the Act.

4.2.5. Copyright Act, 2022

The Copyright Act[29] (hereinafter referred to as the CA) provides for the protection of the intellectual property rights of copyrights owners in literary works, musical works, artistic works, cinematograph films, sound recordings and broadcasts[30]

Section 44 of the CA[31] provides:

> 44 (1) Any person who:
>
> (a) makes or causes to be made for sale, hire or for the purposes of trade or business any infringing copy of a work in which copyright subsists;
>
> (b) imports or causes to be imported into Nigeria, other than for private or domestic use, a copy of any work which, if it had been made in Nigeria, would be an infringing copy; or
>
> (c) has in his possession, any plate, master tape, machine, equipment, device or contrivance for the purposes of making any infringing copy of any such work, commits an offence and is liable on conviction to a fine of at least N10,000.00 for every copy dealt with in contravention of this section or imprisonment for a term of at least three years or both.[32]

Section 38 of the CA further provides:

---

[28] *Ibid.*
[29] Copyrights Act 2022 (Act No. 8).
[30] *Ibid* s1.
[31] *Ibid.*
[32] *Ibid* s44(1)(a)(b)(c).

> 38. (1) In any action for infringement of any right under this Act, where an ex parte application is made to the court, supported with an affidavit, that there is reasonable cause to suspect that there is in any house or premises an infringing copy or any plate, film, device or contrivance used, intended to be used or capable of being used for the purpose of making infringing copies, the court may issue an order as it deems just, authorising the applicant to enter the house or premises at any reasonable time by day or night accompanied by a police officer or a Copyright Officer, to
>
> (a) seize, detain and preserve the infringing copy or contrivance; and
>
> (b) inspect any document, relating to the action, in the custody or under the control of the defendant.[33]

Although, the CA[34] did not directly mention cybercrime, this research however submits that it has bearing on cybercrime especially the section that has to do with plagiarism.[35] As it has been stated in the preceding chapter, one of the types of cybercrime prevalent in Nigeria especially in tertiary institutions is cyber plagiarism which students often engage in.[36] Copy right infringers can be prosecuted under the CA[37] notwithstanding the nature of the infringement whether it is done with a computer over internet connection or manually. The CA makes provision for the seizure of devices and contrivances used in copy right infringement include computer systems.[38]

4.2.6. The Cybercrimes (Prohibition, Prevention ETC) Act, 2015

All the legislations discussed above dealt with offenses that can be considered as cybercrime in inchmeal and not in a comprehensive nature. The dearth of comprehensive legal framework

[33] *Ibid.*
[34] *Ibid.*
[35] *Ibid* s1(a).
[36] U. D. Onuoha and C. N. Ikonne, 'Dealing with the Plague of Plagiarism in Nigeria' [2013] (4) (11). See also <https: //core.ac.uk/download/pdf/234634388.pdf>. Accessed 29th February 2024.
[37] *Ibid* s44.
[38] *Ibid* s38.

informed the need for the enactment of a legislation that will collate all the legal provisions on cybercrime fragmented in different legislations into unified comprehensive legal framework. Towards this end, a bill was proposed on the flow of the Senate in September, 2008 titled "A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for other Related Matters."[39] In May 2015, the bill was signed into law as the foremost legislation in Nigeria that deals specifically with cybercrimes and cyber security defining acts and conducts that constitute cybercrime and prescribing punishments accordingly.

The Cybercrimes (Prohibition, Prevention, ETC) Act,[40] (hereinafter referred to at the Cybercrimes Act) put in place a legal, regulatory and institutional framework for the prohibition, prevention, detection, investigation and prosecution of cybercrimes and for other related matters.

The Cybercrimes Act[41] is made up of 59 Sections, 8 Parts and 2 Schedules. 1st Schedule lists the Cybercrime Advisory Council,[42] while the 2nd Schedule[43] lists businesses to be levied for the purpose of the Cyber Security Fund under section 44 (2) (a).[44] They are: GSM service providers and all telecom companies; Internet service providers; banks and other financial institutions; Insurance companies; and Nigerian Stock Exchange.[45]

The Cybercrime Act[46] which has a nationwide application throughout the Federal Republic of Nigeria[47] sets forth its objectives when it provides that:

The objectives of this Act[48] are to –

[39] A. T. Bello, 'Anatomy of Cybercrime in Nigeria: The Legal Chronicle' [2017] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3055743>. Accessed 29th February 2024.
[40] Cybercrimes (Prohibition, Prevention ETC.) Act 2015.
[41] *Ibid.*
[42] *Ibid.* First Schedule, s42(1).
[43] *Ibid*. Second Schedule.
[44] *Ibid.*
[45] *Ibid.*
[46] *Ibid.*
[47] *Ibid.* s2.
[48] *Ibid.* s1(a)(b)(c).

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

(b) ensure the protection of critical national information infrastructure; and

(c) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

In keeping with its objective of providing an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria, the Act provides series of cyber offences and as well as prescribed punishments accordingly to these offences.

Given the importance of certain aspect of information infrastructure to the economy and the need to preserve them for the smooth running of the economy, the Act commenced its substantive section by empowering the President on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social wellbeing of its citizens, as constituting Critical National Information Infrastructure[49]. The Presidential Order made under subsection (1) of this section[50] may prescribe minimum standards, guidelines, rules or procedure in respect of:

a. The protection or preservation of critical information infrastructure;
b. the general management of critical information infrastructure;
c. access to transfer and control of data in any critical information;

[49] *Ibid.* s3(1).
[50] *Ibid*. s3.

d. infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national information infrastructure;
e. the storage or archiving of data or information regarded critical national information infrastructure;
f. recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and
g. any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure

The Cybercrime Act[51] then went forth to provide for offences against critical national information infrastructure and made it an offence punishable with a term of imprisonment of not less than 10 years without an option of fine for any person who commits any of the offences punishable under the Cybercrime Act against any critical national information infrastructure[52].

Where however, the offence committed under subsection (1) of section 5 results in grievous bodily injury, the offender shall be liable on conviction to imprisonment for a term of not more than 15 years without option of fine.[53] Where the offence committed under subsection (1) of section 5 results in death, the offender shall be liable on conviction to life imprisonment.[54] The punishment attached to these offences are grave given the importance of the infrastructure involved and the extent of chaos that will result if they are tampered with.

The Act went further to provide for the offence of unlawful access to a computer by stating that any person who without authorization or in excess of authorization, intentionally accesses

[51] *Ibid.*
[52] *Ibid.* 5(1).
[53] *Ibid.* 5(2).
[54] *Ibid* .5(3).

in whole or in part, a computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment.[55] Further, where the offence provided in subsection (1) of section 6 is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, the Cybercrime Act prescribes the punishment for imprisonment of term not less than 7 years or a fine of not less than N7,000,000,00 or to both fine and imprisonment.[56] Any person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification with the act or omission, commits an offence and liable on conviction to imprisonment for a term of not less than 7 years or to a fine of not more than N7, 000,000.00 or to both fine and imprisonment.[57]

The Cybercrime Act provided that from the commencement of the Act all operators of a cybercafé shall register as a business concern with Computer Professionals' Registration Council of Nigeria (CPRCN) in addition to a business name registration with the Corporate Affairs Commission. Cybercafés shall maintain a register of users through a sign-in register. This register shall be available to law enforcement personnel whenever needed.[58] Any person, who perpetrates electronic fraud or online fraud using a cybercafé, shall be guilty of an offence and shall be sentenced to three years imprisonment or a fine of One Million Naira or both.[59] The Cybercrime Act went further to provide that, in the event of proven connivance by the owners of the cybercafé, such owners shall be guilty of an offence and shall be liable to a fine of N 2,000,000.00 or 3 years jail term or both.[60]

[55] *Ibid.* 6(1).
[56] *Ibid.* s6(2).
[57] *Ibid.* s6(3).
[58] *Ibid.* s7(1).
[59] *Ibid.* s7(2).
[60] *Ibid.* s7(3).

Next in line is the offence of system interference and its punishment. In criminalizing the act of system interference, the Cybercrime Act[61] provides that any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof from functioning in accordance with its intended purpose, commits an offence and liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000.000.00 or to both fine and imprisonment.[62] The Cybercrime Act further provides for the offence of Intercepting Electronic Messages, Emails, Electronic and Money Transfers. Its provides that, any person who unlawfully destroys or aborts any electronic mails or processes through which money and or valuable information is being conveyed is guilty of an offence and is liable to imprisonment for 7 years in the first instance and upon second conviction shall be liable to 14 years imprisonment.[63] The Cybercrime Act provides for the offence of Tampering with Critical Infrastructure. Its provides that, From the commencement of this Act, any person being employed by or under a Local Government of Nigeria, private organization or financial institution with respect to working with any critical infrastructure, electronic mails commits any act which he is not authorized to do by virtue of his contract of service or intentionally permits, tampering with such computer, is guilty of an offence and is liable to a fine of N2 ,000,000.00 or imprisonment for 3 years.[64]

Section 11 of the Cybercrime Act[65] provides for the offence of Willful misdirection of Electronic Message, section 12 provided for Unlawful Interception,[66] while sections 13 and 14

[61] *Ibid.* s8.
[62] *Ibid*. s8.
[63] *Ibid*. s9.
[64] *Ibid.* s10.
[65] *Ibid*. s11(n40).
[66] *Ibid.* s12 (1)(2)(3).

provide for Computer Related Forgery and Computer Related Fraud[67] respectively. Sections 15 provides for Theft of Electronic Devices[68] while, section 16 provides for unauthorised modification of Computer Systems, Network Data and System Interference.[69] Section 17 provides for forgery of Electronic Signature.[70] Section 18 provides for Cyber Terrorism, the section provides that, any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment. For the purpose of this section, "terrorism" shall have the same meaning under the Terrorism (Prevention) Act, 2011 as amended.[71]

The Act provides for the offence of Identity theft and impersonation punishable with 7 Seven years imprisonment or a fine of not less than N7,000,000.00 or to both fine and imprisonment.[72] These offences are committed where; any person who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft of its employer, staff, service providers and consultants with the intent to defraud; or any person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person; or fraudulently impersonates another entity or person, living or dead, with intent to:

(a) gain advantage for himself or another person;

(b) obtain any property or an interest in any property;

(c) cause disadvantage to the entity or person being impersonated or another person; or

(d) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.[73]

[67] *Ibid*. s13 and s14.
[68] *Ibid.*
[69] *Ibid.*
[70] *Ibid.*
[71] *Ibid*. s18(1)(2). It should be noted there an extant terrorism law in Nigeria which is Terrorism (Prevention and Prohibition) Act, 2022 [sic].
[72] *Ibid*. s22(1)(2).
[73] *Ibid*. s22(3)(a)(b)(c)(d).

Subsection 4 of section 22 provides that, any person who makes or causes to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false and with intent that it be relied upon respecting his identity or that of any other person or his financial condition or that of any other person for the purpose of procuring the issuance of a card or other instrument to himself or another person commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than N7,000,000.00 or to both such fine and imprisonment.[74]

The Cybercrime Act also provides for Child pornography and related offences[75] and further provides that any person who intentionally uses any computer or network system in or for:

(a) producing child pornography;

(b) offering or making available child pornography;

(c) distributing or transmitting child pornography;

(d) procuring child pornography for oneself or for another person;

(e) possessing child pornography in a computer system or on a computer-data storage medium; commits an offence under this Act and is liable on conviction.[76]

The punishment for the mode of commission of the offence as contained in (a), (b) and (c) above is imprisonment for a term of ten years or a fine of not more than N20,000,000.00 or to both fine and imprisonment,[77] while the punishment in respect of those contained in paragraphs (d) and (e) of this subsection, to imprisonment for a term of not more than 5 years or a fine of not more than N10,000,000.00 or to both fine and imprisonment.[78]

[74] *Ibid.* s22(4).
[75] *Ibid*. s23(1).
[76] *Ibid.* s23(1)(a)(b)(c)(d)(e)
[77] *Ibid.* s23(1)(e)(i).
[78] *Ibid*. s23(1)(e)(ii).

The Cybercrime Act went on to define the term "child pornography" to include pornographic material that visually depicts:[79]

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; and

(c) realistic images representing a minor engaged in sexually explicit conduct.

As regards who constitute a child or minor, the Cybercrime Act provides that for the purpose of the section, the term "child" or "minor" shall include a person below 18 years of age.[80]

The offence of Cyber-stalking[81] is further provided for by the Cybercrime Act punishable with fine of not less than N7,000,000.00 or imprisonment for a term of not more than 3 year or to both fine and imprisonment. The offence is deemed committed when any person who, knowingly or intentionally sends a message or other matter by means of computer systems or network that:

(a) is grossly offensive or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

(b) he knows to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to another or causes such a message to be sent; commits an offence under this Act and shall be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.[82]

The Cybercrime Act similarly provides for the offence of Cyber-squatting[83] and further provides that the offence is committed by any person who, intentionally takes or makes, use of a name, business name, trademark, domain name or other word or phrase registered, owned or

[79] *Ibid*. s23(4).
[80] *Ibid.* s23(5).
[81] *Ibid.* s24.
[82] *Ibid.* s24(1)(b).
[83] *Ibid.* s25.

in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user. The punishment is imprisonment for a term of not more than 2 years or a fine of not more than N5,000.000 or to both fine and imprisonment,[84] In awarding any penalty however against an offender under this section, a court shall have regard to the following:

(a) a refusal by the offender to relinquish, upon formal request by the rightful owner of the name business name, trademark, domain name, or other word or phrase registered owned or in use by an individual, body corporate or belonging to either the federal, State or Local Governments in Nigeria or (b) an attempt by the offender to obtain compensation in any form for the release to the rightful owner for use in the internet of the name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Government of Nigeria.

In addition to the penalty specified under this section, the court may make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.[85]

The Cybercrime Act equally provides against Racist and Xenophobic offences.[86] Its provides in it section 26[87] as follows:

Section 26 (1) any person who with intent –

(a) distributes or otherwise makes available, any racist and xenophobic material to the public through a computer system or network,

(b) threatens, through a computer system or network,

[84] *Ibid.* s25(1).
[85] *Ibid*. s25(2)(a)(b).
[86] *Ibid.* s26.
[87] *Ibid*s26(1).

i. persons for the reason that they belong to a group. distinguished by race, colour, descent. national or ethnic origin, as well as, religion, if used as a pretext for any of these factors; or

ii. a group of persons which is distinguished by any of these characteristics;

(c) insults publicly, through a computer system or network -

i. persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or

ii. a group of persons which is distinguished by any of these characteristics; or

(d) distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998; commits an offence and shall be liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than N10,000,000.00 or to both fine and imprisonment.

In addition, the Act offered a definition of the term "racist and xenophobic material" which it stated to mean any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors".[88]

The Cybercrime Act also provides for attempt, conspiracy, aiding and abetting.[89] Its provides that any person who attempts to commit any offence or does any act preparatory to or in

[88] *Ibid.* s26(2).
[89] *Ibid.* s27(1)(2).

furtherance of the commission of an offence under this Act; or abets, aids or conspires to commit any offence under this Act, commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

The Act makes provisions for corporate liability.[90] While, a body corporate that commits an offence under the Act shall he liable on conviction to a fine of not more than N10,000,000. Any person who at the time of the commission of the offence was a director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable on conviction to imprisonment for a term of not more than two years or a fine of not more than N5,000,000 or to both fine and imprisonment[91] so long as the said officer had knowledge and failed to exercise due diligence in the prevention of the offence.[92]

4.3. Institutional and Regulatory Frameworks for Prevention and Control of Cyber Crime in Nigeria

The Cybercrime Act[93] which is the principal legal framework regulating cybercrime in Nigeria did not prescribe any particular law enforcement agency as being responsible for the implementation of the Cybercrime Act. However, Part V of the Cybercrime Act that contains provision for administration and enforcement of the Cybercrime Act provides in section 41(1) to the effect that the office of the National Security Adviser shall be the co-coordinating body for all security and enforcement agencies under the Cybercrime Act.

Section 41 (3)[94] further provides that all law enforcement, security and intelligence agencies shall develop requisite institutional capacity for the effective implementation and

[90] *Ibid*. s27
[91] *Ibid*. 27(2)(a).
[92] *Ibid*.
[93] Cybercrime Act (n40).
[94] *Ibid.* s41(1).

administration of the provisions of the Act. Section 58[95] which is the interpretation section of the Cybercrime Act defines law enforcement agencies to include any agency for the time being responsible for implementation and enforcement of the provisions of the Act.

Further, section 42(1)[96] provides for the establishment of the Cybercrime Advisory Council which shall comprise of a representative each of the ministries and Agencies listed under the First Schedule to the Cybercrime Act. The Cybercrime Advisory Council shall amongst other things have the function of formulating and providing general policy guidelines for the implementation of the provisions of the Act[97]

A community reading of the above provisions of the Cybercrime Act together with the Schedule to the Act shows that the following are the institutional and regulatory agencies charged with the enforcement of the Act:[98]

(a) Office of the National Security Adviser;
(b) Federal Ministry of Finance;
(c) Ministry of Foreign Affairs;
(d) Federal Ministry of Trade and Investment;
(e) Central Bank of Nigeria;
(f) Federal Ministry of Justice;
(g) Department of State Services;
(h) Nigeria Police Force;
(i) Economic and Financial Crimes Commission;
(j) Independent Corrupt Practices Commission;
(k) National Intelligence Agency;
(l) Nigerian Security and Civil Defence Corps;
(m) Defence intelligence Agency;
(n) Defence Headquarters;
(o) National Agency for the Prohibition of Traffic in Persons;
(p) Nigeria Customs Service;
(q) Nigeria Immigration Service;
(r) National Space Management Agency;
(s) Nigerian Information Technology Development Agency;
(t) Nigerian Communications Commission;

[95] *Ibid.*
[96] *Ibid.*
[97] *Ibid*. s43(1)(b).
[98] *Ibid.* s1(1) to the First Schedule of the Cybercrime Act.

(u) Galaxy backbone;
(v) National Identity Management Commission;
(w) Nigeria Prisons Service;

The general role of these agencies is to develop requisite institutional capacity for the effective implementation of the provisions of this Act and shall in collaboration with the Office of the National Security Adviser, initiate, develop or organize training programs nationally or internationally for officers charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.[99]

The Cybercrime Act grants powers to the law enforcement officer authorized by law to apply to court ex-parte for the issuance of a warrant to enter and search premises, conveyance or any person found therein as well as to seize and retain any computer or electronic device and relevant material found in them.[100]

The Cybercrime Act provides for prosecution of offences. Subject to the powers of the Attorney General, relevant law enforcement agencies shall have power to prosecute offences under this Act.[101]

4.4. Challenges in Cybercrime Investigation, Prevention and Control in Nigeria.

Cybercrime as it has been stated it a specie of crime different from other conventional crime reason that it is mostly committed over virtual space.[102] As such, investigation and prevention of cybercrime assumes entirely different approach from that adopted while combating other conventional crimes. Some challenges exist that are peculiar to the investigation and prevention of cybercrime amongst which include the following:

[99] *Ibid*. s41 (3).
[100] *Ibid*. s45.
[101] *Ibid*. s47.
[102] Amrapali Mukherjee, 'Difference between Cyber Crime and Conventional Crime' (2023) <https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in-tabular-form/ >. Accessed 1st of March 2024.

a. **Number of Users:** As observed in chapter one of this work, it is estimated in a study[103] that out of the total population of Nigeria of approximately 200 million, 122.5 million have access to internet services. As at 31st January, 2023 Nigeria's internet penetration rate was 51%.[104] This number no doubt continues to grow exponentially and with this growth in the number of users of the internet comes with an attendant growth of the incidences of crime being committed by the use of the internet. The development of cheap hardware and cheaper subscription fee to access the internet will see the number continue to grow. With the growing number of internet users, the number of targets and offenders equally increase such that even if it is only a small percent of the population is involved in cybercrime the number will be so greatly disproportionate to the number of law enforcement agencies personnel involved in the investigation of cybercrime. Thus, increase in the number of users of internet will cause greater difficulty to law enforcement agencies especially as it is difficult to automate investigation process in Nigerian.[105]

b. **Inadequacy of Legal Framework:** Before the advent of Nigerian Cybercrime (Prohibition, Prevention ETC) Act, 2015 there is no direct law for combating cybercrime, most of the existing laws only made allusion one way or the other to some of the offences under the cybercrime Act and the vacuum gave most of the cybercriminal's opportunity to operate freely without been checkmated for their illicit activities. The success or failure of the Law Enforcement agencies in the performance of their Constitutional duties of detecting crime, preventing crime, apprehending

[103] Internet World Statistics, *Internet Users Statistic for Africa and Internet Penetration in Africa* as at 31st December 2017. <www.internetworldstatsconijstatsl.htrn >. Accessed 1st March 2024.
[104] D. D. Sasu, 'Internet 'Nigeria: online usage Penetration' 2018 to 2027' (2024). <https://www.statista.com/statistics/484918/internet-user-reach-nigeria/>. Accessed 1st of March 2024.
[105] O. V. Chukwuma, I. P. Okolie and A. N. Eneh, 'Automated forensic auditing and fraud control in Nigeria' (2022) *International Journal of Multidisciplinary Research and Growth Evaluation.* <https://www.researchgate.net/publication/366544280_Automated_forensic_auditing_and_fraud_control_in_Nigeria>. Accessed 1st March 2024.

offenders, investigating crime and prosecuting offenders with sole aim of maintaining law and order[106] is wholly dependent on the existing adequate legal framework in place. As technology evolves, new cybercrime will continue to emerge and in order to nip in such crime in the bud, the legislatures who are clothed with the constitutional powers to make laws,[107] must ensure there are appropriate laws in place to confront the new emerging cybercrime by constantly carrying out a periodic review on laws dealing with cybercrimes in Nigeria.[108]

c. **Inadequate Resources:** The success or failure of the Law Enforcement agencies in the performance of their Constitutional duties of detecting crime, preventing crime, apprehending offenders, investigating crime and prosecuting offenders with sole aim of maintaining law and order[109] is also dependent on the number of resources at their disposal. The law enforcement agencies are often incapacitated by inadequate resources in carrying out their mandates in investigating cybercrimes[110]. Investigation of complex crimes like cybercrimes requires collection and preservation of data evidence that will be used in court for effective prosecution of offenders involve and collection and storage of data evidence which most times requires traveling asides the shores of Nigeria involves huge amount of money which our Nigeria investigators involved in cybercrime investigation do not have and this lack of adequate resources limit them and as result they conduct armchair investigation that makes prosecution of cybercrime offender an effort in futility.[111]

d. **Lack of Skilled Personnel:** One of the challenges with cybercrime investigation in Nigeria is that, apart the fact that most of the officers involved in the investigation of

[106] Section 4 of the Nigeria Police Act, 2020 provides for the primary functions of the Nigeria Police Force.
[107] Section 4 of Constitution of the Federal Republic of Nigeria, 1999 as amended.
[108] E. O. C. Obidimma and O. Ishiguzo, 'Cybercrime Investigation and Prosecution in Nigeria: The Critical Challenges' [2023] (8) *African Journal of Criminal Law and Jurisprudence (AFJCLJ),* 30.
[109] Nigerian Police Act (n106).
[110] Obidimma (n108).
[111] *Ibid*,31.

cybercrime are computer illiterates,[112] they have not attended any further training especially on how to investigate crimes like cybercrime that usually occur on virtual world cutting across many countries with most of the offender's identity remaining anonymous and investigating these crimes by most of this officers without the requisite professional training on prevention and investigation of transnational crime and with little or no computer training makes them unable to efficiently conduct a detail discreet investigation in such cases.[113] These unskilled officers also lack the proficiency requires to obtain data evidence from the virtual scene of cybercrime and preserve such digitally obtained data evidence against virus attacks and even if a direct and accurate information is provided to the unskilled investigating officer, he will still not achieve any positive result due his ignorant on the applications of the information and this made tracing criminals online difficult to investigating officers who have little or no knowledge or mechanism of obtain data information.[114]

e. **Extradition or Doctrine of Dual Criminality:** The doctrine of dual criminality is a serious issue in cybercrime investigation.[115] When investigation of such crime involves extradition of the offender and this is because the act or omission necessitating the extradition must have been considered a crime and punishable under the criminal laws of both the surrendering and requesting states because if same act or omission does not constitutes a punishable crime in the two countries, extradition relating to cybercrime will be problematic and as such, a person who commits an offence in Nigeria may not be extradited if his offence is not criminalized in the other state.[116]

---

[112] *Ibid*,31.
[113] *Ibid*,31.
[114] *Ibid*,31.
[115] *Ibid*,32.
[116] M. Waibel and T. Malone, '*Constitutional Protections Afforded to Individuals Subject to an Extradition Request*' [2017] (8)(1) *University of Cambridge Faculty of Law Legal Studies Research Paper Series on SSRN.*

f. **Anonymity Challenge:** Most times the cybercriminals usually conceal their identity using different apps which may include: proxy servers, spoofed email or internet protocol (IP) addresses and the use of anonymity tools by offenders makes digital investigative method of cybercrime difficult for law enforcement agents.[117] The use of different internet apps by cybercriminals to hide their identity will require serious efforts on the part of skilled investigators to trace back their hidden identity.[118] It is always difficult for investigators to unearth the true identity of the criminals who operate in virtual world.[119] Various anonymity services are available on the internet, making it challenging to track down offenders based on their IP addresses. Some anonymity service includes: proxy, virtual private network, and Tor Proxy Services is used to send network traffic through an intermediary computer called proxy servers or an application-level gateway which functions by intercepting connections between the sender and receiver.[120] It channels all incoming data through one port and forwards the rest via another port. It blocks direct access between two networks, making it difficult for a third party to get internal addresses and details of private networks. A Virtual Private Network (VPN) is a tool used to maximize an internet user's privacy and freedom online.[121] A good VPN service allows an internet user to (a) appear to be anywhere in the world by replacing your IP address and location with that of the VPN server, (b) restore your privacy by encrypting your internet traffic and thereby making it unreadable to third parties, such as your internet service provider, network admin,

<https://www.law.cam.ac.uk/press/news/2017/01/legal-studies-research-paper-series-vol-8-no-1>. Accessed 1st March 2024.

[117] Obidimma (n108), 32.

[118] *Ibid.* 33.

[119] *Ibid.* 33.

[120] Proxy Servers, November 2018. <https://kb.iu.edu/d/ahoo.>. Accessed 1st March 2024.

[121] S. Taylor, 'VPN: Every about VPN you need to know, [2019]. <https://restoreprivacy.com/vpn > . Accessed March 2024.

or surveillance agencies, (c) unblock restricted content no matter where you are located in the world.[122]

g. **Encryption Challenges:** Encryption is a technique used to encode communications proceeding transmission to make such communication unreadable if intercepted.[123] Encrypting messages means the use of algorithms to encrypt data to render it unintelligible to third parties who do not have the secret information necessary to decrypt the message.[124] The goal is for the intended recipient who has the key to the message to decode and restore it to its original form. [125] While companies and organizations have legitimately used encryption to secure their transaction data in electronic scheme, cybercriminals and terrorist have also taken advantage of it to guide their fraudulent communication from law enforcement agents.[126] Encryption is achieved by assigning new letters to represent letters previously used in a file, then scrambling the letters to make interpretation significantly more difficult. Encryption software was originally designed for government use to protect files from persons without proper security clearance.[127]

h. **Jurisdictional Challenge:** Cybercrime is an offence that mostly cut across borders. A fraudster in Nigeria may target a victim in Scotland and use a cohort based in Turkey to facilitate and finalize the crime and in situation like this, jurisdiction can be based on different issues such as the actual place the cybercrime was committed, the offender's country of origin, the property and or person affected by the crime. In the virtual environment, the issue of jurisdiction in international and domestic laws has

---

122 *Ibid.*
123 M. Yar, *Cybercrime and Society* (2nd edn, Sage Publication Inc. 2013), 58.
124 P. Gerard and G. Broze, 'Encryption: An Overview of European Policies' [1997] (3)(4). *IT Telecoms and Broadcasting CTLR,* 168.
125 *Ibid.*
126 *Ibid.*
127 *Ibid.*

been raised owing to the de-territorial nature of cyber offences[128]. The ease with which an internet user can access a website anywhere globally had led to the internet being described as multi-jurisdictional. The multi-jurisdictional nature of the internet makes it problematic for courts to determine jurisdiction. Question like whether a particular event in cyberspace is controlled by the laws of the state or country where the website is located, or where the criminal initiated the crime or where the victim resides usually arises during prosecution of crime. The Nigerian Supreme Court in the case of Madukolu v Nkemdilim[129] held that it is settled that jurisdiction is the life blood of any adjudication without which no proceeding, however brilliantly conducted by the Court or Tribunal can be valid.

i. **Prosecution of Cybercrime:** The law provides that relevant law enforcement agencies shall have power to prosecute offences under the Cybercrime Act[130] subject to powers of the Attorney-General.[131] The Attorney-General and it state counterpart have the power to institute, undertake and discontinue criminal prosecution even if they were instituted by any other authority or person.[132] In Ezekiel v Attorney-General of the Federation,[133] the full panel of the Nigerian Apex court held that institution of criminal proceedings against any person before any court in Nigeria other than a court martial is not exclusive preserve of the Attorney-General of the Federation and/or his counter in the State. There are several agencies, bodies and institutions, beyond the Attorney-General of the Federation and/or his counterpart in the state, with powers to prosecute specific offences. This becomes more compelling given the provision of the

[128] G. Shashikala, 'Problems of Jurisdiction in Cyberspace and its Impact on International and Domestic Laws' [2023] <http://shodhganga.inflibnet.ac.in/bitstream/10603/113328/5/chapter%20ii.pdf >. Accessed March 2024.
[129] (1962) 2 SCNLR 34.
[130] *Ibid.* s47 (n40).
[131] *See* sections 174 & 211 of the 1999 Constitution of the Federal Republic of Nigeria that give the Attorney-Generals of Federal and States powers to institute, take-over and discontinue criminal cases.
[132] Ezekiel v A-G Federation (2017) Vol. 266 LRCN 1.
[133] *Ibid.*

Economic and Financial Crimes Commission (Establishment) Act 2004. The Provisions of Sections 7(1) and (2), 13 (1), (2) and (3) of the EFCC Act empowers the prosecutors in the Legal and Prosecution Unit of the EFCC to prosecute any person who commits any of the offences that the Commission is empowered to prosecute under the Act.[134] The court with the requisite jurisdiction to entertain any cybercrime charge in Nigeria is the Federal High Court located in any part of Nigeria, regardless of the location where the offence is committed.[135]

j. **Trained, Poorly Paid and Lack of Protection for Law Enforcement Agencies:** This research is of the opinion that cybercriminals are crass opportunists always looking for avenues to make unlawful wealth or in rare cases wreak havoc to computer systems. They have been described as professional thieves and soldiers of fortunes,[136] above all, cybercriminals are experts in computer and cyberspace issues, thus, the expertise of cybercriminals cannot be juxtaposed with law enforcement agencies who are mere government officials that are ill-trained, poorly remunerated and who offer their services without proper security and protection.[137] The foregoing factors make efforts targeted at investigation and enforcement of cybercrime laws, puerile, because the cybercriminals are far ahead of law enforcement agencies in terms of access to funds and necessary acquisition of skills in computers and cyberspace related issues.[138]

k. **Dearth of Experts in Prosecution of Cybercrimes:** Related to the above factors of poor training, remuneration and inadequate security and protection on the hazardous job for law enforcement agency officials is the dearth of experts in the prosecution of

[134] Shema v FRN (2018) 9 NWLR (Pt 1624 at 337). See also section 66 of the Police Act, 2020 which empowers a Legal Officer with the Police to Prosecute before superior courts.
[135] Cybercrime Act, s50(1-4).
[136] Legal Brief, E-Law & Management, [2015] (1581) *Cyberlaw & Technology*,1.
[137] Obidimma (n108), 34.
[138] *Ibid.* 33.

cybercrimes.[139] It is a well-known fact that, even if the law enforcement agencies had done a good job in the investigation of cybercrime, at the litigation stage, expertise of prosecution attorneys is still very important to secure the conviction of cybercriminals as it is incumbent on prosecution to proof his case beyond doubts; unfortunately, this is not the case as there is dearth of savvy prosecutors in government justice departments,[140] however, cybercriminals have unfettered access to renown private attorneys who charge very high legal fees which is not a problem to the cybercriminals as they could readily afford to pay high professional fees to lawyers who specializes in cybercrime practice; further, anonymity issue of cybercriminals and the nature of evidence which more often than not are tenuous, regarding the fact that investigators can only rely on traces and tracks left on computers and Internet.[141] All these go to compound the case of prosecutors who are not as grounded in handling of cybercrime litigation compared with their counterparts in private practice; these identified gaps unfortunately are a plus for cybercriminals who in addition to technicalities in cybercrime cases have more than enough funds to hire first class attorneys.

l. **Lack of Effective Reporting and Dearth of Data:** As earlier pointed out before now that many countries in the world have applicable law and policy against cybercrime but the enforcement of same is a challenge and part of the challenge is not unconnected with lack of effective reporting mechanism of incidences of cybercrime to the appropriate authorities across the globe,[142] in effect, this development has militated against bringing to global attention and appreciation of the extent of the menace of cybercrimes; closely related to reluctance to disclosure of cybercrime is the lack of cooperation on the part of the victims, other stake holders and witnesses with police

[139] *Ibid*. 34.
[140] *Ibid*. 34.
[141] *Ibid*. 34.
[142] *Ibid*. 35.

or other agencies saddled with investigation and prosecution of cybercriminals, it is immaterial whether private, corporate or institutional entities are the victims. [143] Lack of effective reporting of cybercrime events and dearth of data go *pari passu*. This research submits that it is when cybercrimes are reported that data about same can be collated and published. The dearth of reliable data and information generally about cybercrimes have created lack of awareness, the said development has shrouded the extent of the problem to which mankind is presently faced with.[144] This research is of the view that the awareness and appreciation of any problem in human endeavors is the beginning of solving the problem, as things stands today, only a fragment of the elite are aware of the impact of cybercrimes on the society.[145]

4.5. Approaches of other Jurisdictions towards Prevention and Control of Cyber Crime.

Cybercrime is a transnational global phenomenon affecting most countries in the world, developed and developing alike.[146] Despite the fact that cybercrime has long historic antecedents, no nation yet including the tech savvy one cannot claim to have been successful in completely eradicating the menace of cybercrime as this is not feasible at the moment.[147] However some technologically advanced countries like the United States of America and the United Kingdom have in place a more effective system of combating cybercrime than others.[148] The UK has a well-articulated policy and strategy towards combating cybercrime. The UK City of London Police has developed a model strategy to approach cybercrime and reduce the risk

[143] *Ibid.* 35.
[144] *Ibid.* 35.
[145] *Ibid.* 35.
[146] C. Russu 'The impact of low cyber security on the development of poor nations' [2022]. <https://www.developmentaid.org/news-stream/post/149553/low-cyber-security-and-development-of-poor-nations >. Accessed 1st March 2024.
[147] D. Lipton 'Cyber security: Threats Call for a Global Response' [2020]. <https://www.imf.org/en/Blogs/Articles/2020/01/1 3/blog-cybersecurity-threats-call-for-a-global-response>. Accessed 1st March 2024.
[148] UK and US Develop New Global Guidelines for AI Security [2022]. <https://www.ncsc.gov.uk/news/uk-develops-new-global-guidelines-ai-security>. Accessed 1st March 2024.

occasioned there from.[149] This model is popularly known as the Four Ps Model Comprising of; Protect and Prepare[150]. This strategy is developed both as a proactive measure before the commission of cybercrime (Protect and Prevent) as well as a reactive measure after the commission of cybercrime (Pursue and Prepare). The Four Ps will now be considered in more details:

a. **Protect:** This is a proactive measure aimed at preventing the occurrence of cybercrime. This measure is targeted at potential victims of cybercrime including individuals and businesses by raising their level of awareness of the existence of and forms of cybercrime in the first place and educating them on strategies they can employ in protecting themselves from falling victim of cybercrime. Both the government, the police and private establishments have a role to play under this measure in protecting individuals and victims from falling into the hands of cybercrime criminals. The government through campaigns ensures a general basic level of awareness. The police can offer additional insight and guidance on protective measures against cybercrime for individuals and businesses.[151] Under the 'Protect' measure, private ICT companies can beef up the security of their products for better protection of end users of their products for example through compulsory built-in antivirus with automatic updates, making the secure option the default option work on its own[152] etc. Financial institutions like banks can also enhance greater protection for their customers for example by making encrypted online banking and communication a compulsory precondition for online banking.[153]

[149]M. Levi and others, 'The Implications of Economic Cybercrime for Policing' [2015] *Research Report City of London Corporation.*
[150] Cardiff University 'The Implications of Economic Cybercrime for Policing' [2015]. City of London Corporation. <www.cityoflondon.gov.uk/business/researchpublications>. Accessed 1st March 2014.
[151] *Ibid,* 56.
[152] *Ibid,* 56.
[153] *Ibid,* 57.

b. **Prevent:** The 'Prevent' strategy is also a proactive mechanism towards preventing cybercrime from occurring in the first place. 'Prevent' unlike 'Protect' that targets potential victims targets potential criminals[154] and is aimed at attempting to divert potential criminal from engaging in or committing cybercrimes[155]. Under this measure, the internet is monitored and potential criminals identified usually from their role in chat rooms, social media and other of internet presence.[156] From constant monitoring of identified potential criminal when evidence suggests that they may be reaching a serious threshold, then some interruption may be attempted to dissuade and divert these individuals with high risk of engaging in cybercrime.[157] Raising awareness also plays a role in this prevent strategy by educating the public on the risks that are inherent in engaging in cybercrime. The Police however do not do this alone but partners with other organizations such as school or community-based initiatives. This partnership helps in reducing significantly staff input on the part of the police and assist in reaching a wider spectrum of people.[158]

c. **Prepare:** The Prepare' strategy unlike the preceding two discussed is reactive in that it focuses and comes into play in the aftermath of cybercrime.[159] This measure entails in essence planning and preparing for attacks by building post event resilience to reduce the impact of cybercrime as well as improve resilience for future prevention. According to the Scottish Government,[160] this measure involves several aspects including taking those actions or steps to mitigate and respond to cyber threat and

[154] *Ibid*, 57
[155] C. Jones, 'How do 'We' Police Cyber' [2015]. <serocucybercrimeunit@thamesvalley.pnn.police.uk>. Accessed 1st March 2024.
[156] *Ibid*, 57.
[157] *Ibid*, 57.
[158] *Ibid*, 58.
[159] *Ibid*, 58.
[160] Scottish Government, 'Consultation on Proposal for a Cyber Resilience Strategy for Scotland' []2015]. < https://consult.gov.scot/cyber-resilience-policy-team/cyberconsultation/user_uploads/cyber-consultation-june-2015_final.pdf>. Accessed 1st March 2024.

being able to prepare for, adapt to withstand and rapidly recover and learn from disruptions caused by cybercrime. In order to mitigate the impact of a cyber-attack, there is need to have in a place a risk management approach that involves thinking strategically and preemptively[161]. Also, under the "Prepare" intervention, individuals who have fallen victim of one form of cybercrime or the other are identified and encouraged to improve their security and resilience so that they will not suffer repeat victimization. As stated earlier, this awareness measure can be undertaken or supplemented by peer or community level organization.

d. **Pursue:** The 'Pursue mechanism is reactive in nature in the aftermath of cybercrime.[162] It consists in essence of going after cybercriminals with the aim of disruption and prosecuting them. This conforms to the traditional role of the police function as with other conventional crimes. While the "Protect", "Prevent" and "Prepare" dimensions of the Four Ps Model offer the police a minor role especially due to resource constraints as well as because these roles can he undertaken by other institutions, the "Pursue" intervention on the other hand constitute the bulk of the police role.[163] This function is however dependent on victims reports of cybercrime in the private and public sectors to the police.

The above strategy adopted by the UK in combating cybercrime though may have it shortcomings, helps to provide enforcement agencies and other stake holders with a definite, well-articulated policy direction and defined roles in combating cybercrime.[164] This strategy allows for coordination amongst different stakeholders and reduce cost of policing It is the view of this research that, if the Four Ps strategy is adopted with holistic approach with a strong

[161] Cardiff (n150),58.
[162] *Ibid*, 59.
[163] *Ibid*, 59.
[164]J. Saunders 'Tackling cybercrime – the UK response' [2017] (2)(1) <https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1293117>. Accessed 1st March 2024.

will on the part of the government same could equally be effective in combating cybercrime in Nigeria as being used in the UK.

The United State of America is another tech savvy country that is very advanced in combating cybercrimes. Several measures have been adopted by the government of the US in checking the activities of both domestic and international cybercrime criminals. Amongst the prominent of these measures include:

a. **Online Reporting Mechanism:** The US has developed in its fight against cybercrime by creating an online portal through which cybercrime related complaints can be filed.[165] This the US government did through the establishment of the Internet Crime Compliant Center (1C3). The 1C3 was established as a partnership between the FBI and the National White Collar Crime Center (NW3C) to receive internet-related criminal complaints and to further research, develop, and refer the criminal complaints to national, state, local, or international law enforcement and or regulatory agencies for any investigation.[166] This approach allows for greater convenience in reporting occurrence of cybercrime by victims and will lead to increase in the number of reported crime, given the ease with which a complaint can be lodged from the comfort of one's home.[167]

b. **Training and Awareness:** The US in its fight against cybercrime has taken practical steps and multiple initiatives to train its law enforcement agencies to be up-to-date as regards technical knowhow in the investigation and prevention of cybercrime.[168] Further it has undertaken programs to raise awareness of the public on cyber security.

[165] Internet Crime Complaint Centre (IC3).< https://www.ic3.gov>. Accessed 1st March 2024.

[167] Ernst & Young LLP 2015 Strategic National Measures to Combat Cybercrime: Perspective and Learning's for India [2015] <https://www.ey.com>vwLUAssest>ey-strategic-national-measures-to-combat-cybercrime.pdf>. Accessed 1st March 2024.

[168] America's Cyber Defense Agency, 'combatting Cyber-crime' <https://www.cisa.gov/combatting-cyber-crime>. Accessed 1st March 2024.

Some of these initiatives include: The National Cyber Security Awareness Month[169] (under the brand of Stop. Think. Connect.); National Initiative for Cyber-security Education (NICE)[170]; National Cyber-security Education Council (NCEC); Cyber-security Education and Training Assistance Program (CETAP).[171]

4.6. International Framework for Prevention and Control of Cybercrime.

4.6.1 United Nations Office on Drugs and Crimes.[172]

The United Nations has undertaken several important approaches to address the challenge of cybercrime. While in the beginning its response was limited to general guidelines, the organisation has in recent times dealt more intensively with the challenges and legal response. UNODC's goal is to make the world safer from drugs, organised crime, corruption and terrorism by combating these threats to achieve health, security and justice for all and by promoting sustainable peace and well-being.

4.6.2. Council of Europe Convention on Cybercrime 2001.[173]

[169] United States Cyber Security Awareness Month, it is usually observed every October each year. <https://www.nist.gov/cybersecurity/cybersecurity-awareness-month#:~:text=2023%20marks%2020%20Years%20of,safer%20and%20more%20secure%20online>. Accessed 1st March 2024.

[170] The National Initiative for Cybersecurity Education (NICE) is a partnership between government, academia, and the private sector focused supporting the country's ability to address current and future cybersecurity education and workforce challenges through standards and best practices. NICE is led by the National Institute of Standard and Technology (NIST) in U.S. Department of Commerce. <https://en.wikipedia.org/wiki/National_Initiative_for_Cybersecurity_Education> Accessed 1st March 2024.

[171] The Cybersecurity Education and Training Assistance Program (CETAP) was launched to support the Cybersecurity and Infrastructure Security Agency's (CISA) efforts in building and strengthening a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education, including by providing foundational cybersecurity awareness and literacy, encouraging cybersecurity career exploration, and supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

[172] The United Nations (UN) is an international organization founded in 1945.

[173] The Preamble to the Council of Europe Convention on Cybercrime. The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European regions. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

The Council of Europe is playing an active role in addressing the challenges of cybercrime. In 1976, the Council of Europe highlighted the international nature of computer-related crimes and discussed the topic at a conference dealing with aspects of economic crimes. This topic has since remained on its agenda.[174] In 1985, the Council of Europe appointed an Expert Committee to discuss the legal aspects of computer crimes.[175] In 1989, the European Committee on Crime Problems adopted the "Expert Report on Computer-Related Crime", analysing the substantive criminal legal provisions necessary to fight new forms of electronic crimes, including computer fraud and forgery.[176] The Committee of Ministers in 1989 adopted a recommendation[177] that specifically highlighted the international nature of computer crime. In 1995, the Committee of Ministers adopted another recommendation dealing with the problems arising from transnational computer crimes.[178] Guidelines for the drafting of adequate legislation were summarized in the Appendix to the Recommendation.[179]

4.6.3. ECOWAS Directive on Cybercrime

In West Africa, the threat of cybercrime has been acknowledged, and the community has developed a directive, to control cybercrime within its member states. The Draft Directive is an important step in the fight against cybercrime within ECOWAS. In this context ECOWAS did not limit its approach to an improvement of the cooperation within ECOWAS. Instead by aiming to bring its legislation in line with international standards it also went further with regard to the expansion of a foundation for international cooperation. Taking into account the

[174] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.
[175] The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD. Source: Information Technology Crime, 577.
[176] Ibid.
[177] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.
[178]Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.
[179]The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.

international dimension of cybercrime the approach reflects the trend towards global harmonization.[180]

4.6.4. African Union Convention on Cyber Security and Personal Data Protection 2014

This convention was adopted at the 23rd Ordinary Session of the Summit of the African Union (AU) which was concluded in Malabo, Equatorial Guinea on June 27th 2014. The convention addressed three main areas that are often seen[181] as either not regulated or substantially dealt with by the governments in the region: (1) electronic transactions, (2) personal data protection, (3) cybersecurity and cybercrime.[182] It further enjoins state parties to prohibit any data collection and processing, without consent, that reveals racial, ethnic and regional origin, parental affiliation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject, except under certain exceptional circumstances.[183]

Finally, on this chapter, this research submits that Nigeria can take a leaf from the approach adopted in the UK especially as it regards enlightenment of its citizens on the existence of forms and appearances of cybercrime as well as strategies through which individuals and businesses can be safeguarded from cybercrime similar to the 'Protect'. Enlightenment campaigns can be organized, radio jingles and advertisements can be created to educate the populace on the risk of cybercrime and ways of safeguarding oneself from falling victim. Partnership with local and community-based initiative can be created to reach a wider spectrum

---

[180] U. J. Orji 'An Inquiry into the Legal Status of the ECOWAS Cybercrime Directive and the Implications of its Obligations for Member States' [2019] (35) (6) *Computer Law and Security Review.*

[181] P. Tentena, 'Tackling the challenges of cybersecurity in Africa' [2014] (2) *Policy Brief, NTIS.* <http://www.uneca.org/sites/default/files/uploads/ntis_policy_brief_1.pdf >. Accessed 1st March 2024.>

[182] See Articles 2, 8, 24, 25 and 26 of African Union Convention on Cyber-security and Personal Data. <https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html.>. Accessed 1st March 2024.

[183] A. T. Bello 'Anatomy of Cybercrime in Nigeria: The Legal Chronicle [2017]. <http://www.newsfromafrica.org/newsfromafrica/articles/art_14335.html > . Accessed 1st March 2024.

of individuals in the enlightenment campaign. Similarly, Nigeria can incorporate the 'Prevent' approach of the UK by targeting institutions and organizations that have a significant concentration of youths and young person's such as schools in order to launch programs that will dissuade the youths from engaging in cybercrime.

Nigeria can equally incorporate the online reporting mechanism employed in the US to ease reporting procedure of cybercrime in the country so as to increase the number of cybercrimes reported and assist security agencies in going after individuals and criminal organizations engaged in cybercrime in the country. It is the opinion of this research that Nigeria should domesticate international treaties and conventions that will strengthen her preventive and combative measures against cybercrime.

CHAPTER FIVE
CONCLUSION

5.1. Summary of Findings

The advancement in technology has gained universal acceptance which has made the use of computer system and the internet almost unavoidable in today's world. Most of the facets of all human activities which include but not limited to; banking, health, commercial, media, education, entertainment etc. are now internet based. However, this progressive and welcoming development of the internet has also come with its adverse effect caused by the growing rate of internet-related crimes – called "Cybercrime". The increasing rate of cybercrimes in Nigeria has been linked with lack of sufficient laws and failure of the relevant law enforcement agencies to implement the existing laws which is aimed at preventing and combating this crime in Nigeria. A careful examination of these laws shows that there are gaps that needed to be filled if the battle against cybercrime is to be won. Beyond the theories behind why people engage in criminal activities as examined in this research which applies to crime and deviant behaviours generally, several factors underlie the reasons. In essence, this research finds that:

a. One of the major causes of cybercrime in Nigeria is Unemployment and youth restiveness. This is because most offenders are driven into this act due to lack of employment for graduates from secondary and tertiary institutions in Nigeria. It is a notorious fact that a significant number of Nigerian youths including graduates are not gainfully employed while others are under employed. This scourge of unemployment luminously contributes in influencing these youths to engage in criminal activities in general and cybercrime in particular.

b. This research also finds that poverty is another cause of cybercrime in Nigeria, where 40% of Nigerians live below the World Bank's threshold of less than US$1 per day. Poverty is the deprivation of basic resources that are necessary for maintaining the quality of life in terms of food, clothing, shelter and other rights and resources that can

impinge on living conditions and guarantee human dignity. The rate of poverty in Nigeria is alarming as such many cybercriminals engage in cybercrime out of desperation and in an attempt to survive.

c. Cybercrime usually require low financial outlay to perpetrate when compared to some other conventional crimes. With as little as a cell phone or a laptop that has internet connection, one can easily commit crimes over the internet in different parts of the world.

d. The research further finds that Cybercrimes are usually hard to detect due to the fact that they can be committed remotely without the requirement of physical presence of the criminal. Thus from the comfort of one's sitting room, one can conveniently commit cybercrime in any part of the world. The sophisticated devices used by professional and advanced cybercriminals also reduce the chance of being detected by security outfits which most times cannot match the sophisticated devices and implements employed by these cybercriminals.

e. Cybercrime can also be committed out of revenge maybe by vengeful past employees who feel that they have been ill-treated. They therefore commit these offences as a way of getting back at their employer. These past employees can easily access the data base of their previous organization and commit these offences due to the fact that they may have the pass codes which most organizations hardly change even after retrenching some of their staff.

f. Another major finding of this research is that before the advent of Nigerian Cybercrime (Prohibition, Prevention ETC) Act, 2015 there was no direct law for combating cybercrime, most of the existing laws only made allusion one way or the other to some of the offences under the cybercrime Act and the vacuum gave most of the cybercriminal's opportunity to operate freely without been checkmated for their illicit

activities. The success or failure of the law enforcement agencies in the performance of their constitutional duties of detecting crime, preventing crime, apprehending offenders, investigating crime and prosecuting offenders with sole aim of maintaining law and order is wholly dependent on the existing adequate legal framework in place. As technology evolves, new cybercrime will continue to emerge and in order to nip such crime in the bud, the legislatures who are clothed with the constitutional powers with the power to make laws, must ensure there are appropriate laws in place to confront the new emerging cybercrime by constantly carrying out a periodic review on laws dealing with cybercrimes in Nigeria.

g. Another motivating factor that influences people to engage in cybercrime is the low rate of conviction in respect of this class of offence. Conviction coupled with certainty of punishment is usually used as instrument of deterrence to prospective criminals from engaging in a criminal conduct since a rational person will avoid a conduct once he envisages the inescapable consequences of such.

h. Greed or get rich quick syndrome where youths want to jump the legitimate way of acquiring wealth which may take considerable time in favour of perceived quicker ways of acquiring wealth contribute in influencing people to engage in cybercrime of all sorts.

i. The Nigerian society tends to celebrate the rich and shun the poor. People who are wealthy receive respect and acknowledgment from the society without any consideration whatsoever of the source of their wealth. Thus people go out of their ways to engage in all sorts of inconceivable corrupt acts in order to acquire wealth with the assurance that there will be no form of stigmatization from the society as regards the source and means through which their wealth is amassed.

j. Yet some cybercriminals engage in cybercrime out of their perceived sense of justice. These individuals believe that the rich and influential especially the politicians engage

in corrupt practices, embezzle public funds and get away with it since they are seen as being above and the reach of the law, they, therefore assume the responsibility of dispensing their own form of "justice" by targeting these perceived corrupt and rich politicians for their criminal activities. These cybercriminals thus do not consider their actions as constituting an offence rather they believe that they are redistributing resources and dishing out justice to those that are beyond the reach of the law.

k. Pressure from deviant peer groups can equally cause an individual to engage in cybercrime. These individuals especially youths and adolescents in attempt to secure the approval of their peers and have a sense of belonging within their unit as well as to gain respect engage in one sort of cybercrime such as hacking, software piracy, illegal streaming of videos and music.

l. Another cause of cybercrime is negative role modeling. When criminals that engage in cybercrime are viewed by the youth as their role model, they will try to imitate the lifestyle of these criminals and may end up getting involved in cybercrime.

m. Some parents accept gifts above the means of their children without asking the source of the money spent on such gifts. A good number of them are aware of their children's involvement in internet fraud but rationalize it by claiming that it is a way of recovering our national wealth from our colonial masters.

5.2. Recommendations

Cybercrime is a great threat to the Nigerian economy and even to its national peace and security. This study has shown that the abuse of computer technology threatens national security, public safety and even devastates the lives of affected individuals. However, Nigeria like most African countries has a weak legal framework and a weak legal enforcement to effectively combat cybercrime. As shown in this research, the legal framework regulating cybercrime in Nigeria is not as comprehensive like other developed jurisdictions particularly

in reference to the UK and US jurisdictions. The Nigerian legal system in this regard, though above average, still has certain loopholes as already identified in this research. Below are the discussions of the various recommendations towards addressing the challenges identified above:

a. **Legal Frameworks with Constant Review:** Legislations relating to cyberspace and cybercrime must be enacted with much precision in order to deal effectively with the acts of the cybercriminals. Information technology professionals should be involved at the law-making process so as to help make laws that would be in line with the extant level of technology. It is recommended that there should be constantly review of cyber laws so as not to become obsolete. This is in view of the fact that the internet will continue to evolve and with its evolution comes new forms, appearances and waves of cybercrime.

b. **Creation of a Central Agency for Cybercrime:** The government should establish units or bodies charged with directing and developing the investigation and prosecution of the different forms of cybercrimes and to provide them with the necessary human, financial, and technical resources to comply with their obligations in an efficient, effective, and expeditious manner in Nigeria.

c. **Training of Law Enforcement Agencies:** This research is of the opinion that cybercriminals are crass opportunists always looking for avenues to make unlawful wealth or in rare cases wreak havoc to computer systems, they have been described as professional thieves and soldiers of fortunes, above all, cybercriminals are experts in computer and cyberspace issues, thus, the expertise of cybercriminals cannot be juxtaposed with that of law enforcement agencies who are mere government officials that are ill-trained, poorly remunerated and who offer their services without proper security and protection from government. It is recommended that government should

make provision for intensive training and retraining of law enforcement agencies on ICT to be able to track down cyber criminals. This training will enhance investigation of cybercrime, collection and collation of relevant pieces of evidence as well as the prosecution of suspected offenders of cybercrime.

d. **Recruitment of Skilled Personnel:** Skilled law enforcement personnel are the need of the moment, considering the highly technical and advanced nature of cybercrime being reported. To gear up speed in preventing and combating cybercrime, there is a need to engage more cybercrime investigation professionals. Such personnel may be deployed at state level with access to dedicated laboratories for analysis at each state. Such teams also need to be part of the police team investigating cybercrimes.

e. **Engagement of Expert in Prosecution of Cybercrimes:** Related to the above factors of poor training, inadequate security and protection on the hazardous job for law enforcement agency officials is the dearth of experts in the prosecution of cybercrimes. It is a well-known fact that, even if the law enforcement agencies had done a good job in the investigation of cybercrime, at the investigation stage, expertise of prosecution attorneys is still very important to secure the conviction of cybercriminals as it is incumbent on prosecution to proof its case beyond doubts; unfortunately, this is not the case as there is dearth of savvy prosecutors in government justice departments. however, cybercriminals have unfettered access to renowned private attorneys who charge very high legal fees which is not a problem to the cybercriminals as they could readily afford to pay high professional fees to lawyers who specializes in cybercrime practice.

f. **Online Reporting System of Cybercrime:** In order to increase the rate of reporting cybercrime, it is important to have provisions for online reporting of cybercrimes. Using this system, an online cybercrime complaint can be made by the victims of

cybercrime anywhere he she is. They will gain access to a convenient and easy-to-use reporting mechanism that alerts law enforcement authorities of suspected criminal or civil violations. Also, it will provide a central repository for reference to law enforcement and regulatory agencies at the national, state and local level.

g. **Adoption of Definite Strategy:** In addition to the existing legal mechanisms, a strategy needs to be adopted and documented, which states the vision, objective and approach for cybercrime prevention. The strategy and execution of cybercrime security needs to be developed with clear vision for addressing challenges relating to cybercrime in the short term and mid-term with possible review mechanism for a long-term approach in this domain. The global practices from advance law enforcement organizations, such as the Federal Bureau of Investigation (FBI) and the Interpol need to be leveraged and adopted as per their feasibility as part of the country's cybercrime strategy.

h. **Public Enlightenment:** The Government should also provide a well-defined and articulated citizen awareness programs aimed at preventing cybercrime as a proactive basis. This can be achieved through the use of multiple media, such as; print, social, radio and the internet to ensure dissemination to a wider spectrum of the public with the use of local and national languages. Cybercrime awareness can also be introduced in academics in the early stages of education as a mandate for all students in both public and private schools and same must be keenly monitored by the government for strict adherence.

i. **Usage of Strong Password:** Internet user should always use strong passwords that are long in length and which comprise a combination of alphabets, numbers, symbols and punctuation signs. The longer the password the more difficult for it to be guessed or hacked. Internet users should also avoid using as password obvious facts about themselves such as; their names, date of birth, house address, office address and certain

facts along that line. Internet users also, should be weary in disclosing their passwords to unknown persons. Preferably, passwords can be constantly revised and changed overtime. Revision of passwords is essentially important for organizations in that it makes it impossible for persons who are no longer staff of the organization to have access codes to the organization's sensitive information.

j. **Central Database:** A centralized database of suspects, investigations as well cybercriminals should be maintained so that potential criminals as well as criminals may be monitored. Such checks will discourage cybercriminals from engaging in spurious activities in cyberspace. Many countries, such as the USA and the UK has maintained a central repository of cybercriminals and this has helped in monitoring the activities of cybercriminals and prevention of potential criminals from committing cybercrime in the country. That is why in the UK for instance, before you are employed both in public or private organisations, the employee must be mandated to undergo a Disclosure and Barring Service (DBS) check which is one of the requirements to gain employment. It is only a legal regime that has centralized database that can disclose an individual criminal record.

k. **International Cooperation:** The Nigerian government need to promote international cooperation and collaboration with other tech savvy countries in view of the fact that cybercrime is a transnational phenomenon. This will help in not only adopting the best practices by other countries for prevention and combating cybercrime, but also in increasing the capability, knowledge, training, skills, capacity and expertise of cyber security task forces. Additionally, it will help to reduce the harm caused to businesses, customers and citizens due to international cyber-attacks.

l. **Harmonisation of Descriptions of cybercrimes:** As much as possible descriptions of cybercrimes should be harmonized to prevent criminals from taking advantage of

differences between jurisdictions and ensure that all applicable local legislations are complementary to and in harmony with international laws, treaties and conventions.

m. **Poverty Alleviation and Employment Generation:** since unemployment and poverty are cited as some of the root causes of involvement in cybercrime, creation of employment and alleviation of poverty will go a long way in reducing the increase in the rate of cybercrime. It is therefore recommended that government should launch poverty alleviation campaigns targeted at and which will benefit the poor. Furthermore, government should engage in massive employment generation schemes in order to reduce the spate of unemployment in the country. Citizens should also be encouraged to be self-reliant and self-employed since it is obvious that no government can provide jobs for all its citizens.

5.3. Contribution to knowledge

Following the recognition that the internet is not amenable to positive use only but is equally susceptible to abuse by its users and given the extent and gravity of damage that can result from cybercrime, nations have continued to devise approaches and strategies of combating the scourge. In view of the undeniable fact that Nigeria is not immune to cybercrime, it is imperative to state that the conduct of this research will contribute to knowledge in the following areas which will be of immense significance to the following inexhaustible class:

a. This research work serves to enlighten the government on the impacts and effects of cybercrime on the economy of the country as well as on the reputation of the country in the international community. The recommendations as regards approaches adopted by other jurisdictions both legislative and administrative will further provide lessons to be garnered by the government towards curbing the menace of cybercrime in the country.

b. This research work provides a strong knowledge base to security agencies as regards the typology of cybercrime in the country, the root causes driving the involvement of individuals in the commission of cybercrime, the methodology adopted by cybercriminals in perpetrating and perpetuating cybercrime and approaches adopted by other jurisdictions towards the prevention and control of cybercrime.

c. This research work equally contributed to knowledge by showing that Nigeria is not lacking in cyber laws but that the existing laws are inadequate to meet modern realities considering the dynamics in cybercrime. Hence there is the need to amend the existing laws to suit modern trends that will make cybercrime unattractive for cybercriminals. This research work will further serve as a foundation/springboard and reference point for subsequent researchers in this field.

5.4. Areas for Further Studies

Although this study has several strengths, there were also a few limitations. During the course of this research, it was observed that most victims of cybercrime (especially in the banking and financial sectors) are not aware of their rights as consumers under the cybercrime Act. Unfortunately, this work did not dwell on the "rights of victims of cybercrime in Nigeria". This is one area that further research can be developed upon. Secondly, as a result of the limited scope of this research, the researcher never averted his mind to the issue of adequacy of compensation to victims of cybercrime in Nigeria would have also been considered. And lastly, the issue of legal framework for certainty of punishment for cybercrime in Nigeria will also constitute an issue for further research.

5.5. Conclusion

There is no single embracive explication to account for the exhibition of deviant behaviour and human involvement in criminal activities. A lot of factors including; biological, psychological

and sociological may account for this. These factors and a combination of them differ in their application to different individuals in different cultural background and at different dispensations. Cybercrime defined as a crime committed using the instrumentality of a computer and most times internet connectivity, with the computer as either a tool or target may equally result by an interplay of these factors. Since crimes in general and cybercrime in particular is an inevitable consequence of social interaction, efforts then ought to be concerted in adopting measure through which individuals and organizations may protect themselves against being a victim of cybercrime through adopting cyber security measures.

The scourge of cybercrime together with the growing incidence of same is caused by an interplay of several factors prominent amongst which is the high incidence of poverty in the country as well as surge of graduate's unemployment especially amongst the youth. These two predominant factors continue to contribute to the exponential growth of cybercrime industry in Nigeria which leaves in its trail a plethora of negative impacts that go beyond the financial losses of individuals and organizations directly involved as victims of the menace of cybercrime to affect the nation as a whole. Although, Nigeria has taken a commendable step by enacting the Cybercrime Act to protect internet consumers, there is still need for further responses as highlighted in this work. In particular, it will be helpful for Nigeria to consider drawing lessons from the highlighted examples of legal regimes in the United States America and the United Kingdom in order to strengthen the protection of consumers that use electronic banking and payment services where fraud related cybercrime frequently occurs.

More importantly, the Nigerian Cybercrime Advisory Council which is established under section 42(1) of the Cybercrimes Act has powers to formulate guidelines for the implementation of the Act. In this regard, the Council can make guidelines that will impose a greater or strict liability regime on banks and financial institutions under section 19(3) of the

Cybercrimes Act, so that they can have a higher degree of liability for the breach of consumer data.

This research therefore concludes that despite the existence of a legal framework (although weak) regulating cybercrime, there exists challenging factors that hampers the investigation, prevention and control of cybercrime in Nigeria such as; dearth of human and capital resources, lack of trained security personnel, high rate of unemployment, poverty etc. must be addressed headlong. Nigeria can however borrow a leaf from other technologically advanced jurisdictions such as the United States of America and the United Kingdom by incorporating some of the approaches and mechanisms adopted by these tech-savvied countries in her fight against cybercrime. Finally, the National Orientation Agency (NOA) needs to refocus its agenda aimed at debriefing Nigerians, especially the youth, on the dangers of cyber criminality.

BIBLIOGRAPHY

BOOKS

Akpoghome T. U and Umahi O. T. and Nwano T. C., Mapping the Contours of Legal Research Writing and Documentation in Nigeria (University of Nigeria Press Ltd 2nd ed. 2020), 47.

Beccaria C., *Crimes and Punishments*, translated by H. Paolucci, (Bobbs-Merrill1. New York .963).

Clough J., 'Principles of Cybercrime' (Cambridge University Press 2010), 112.

Cohen A. K., Delinquent Boys: The Culture of the Gang (Free Press Glencoe 1955).

Conklin J. E., Criminology (9th edn, Pearson Boston 2007), 315.

Denning D. E., Information Warfare and Security. (ACM Press, USA1999).

Doldovaya A. I., *Criminology: University Textbook* (3rd edn. Moscow. Norma 2005), 510-511.

Durkheim E., *Suicide.* (Free Press. Ney York 1951).

Eysenck H. J., *Crime and Personality* (Houghton Mifflin. Boston MA. 1964).

Gasiokwu M. O., Legal Research Methodology and Project Writing (Jos – Nigeria; Fab Education Books, 1994)

Goddard H. H., *Feeble-mindedness* in D. 3. Shoemaker (ed.) *Theories of Delinquency: An Examination of Explanations of Delinquent Behavior* (Oxford University Press. New York 2005).

Halsbury Laws of England London (Butterworth 2016).

Hare R. D., *Psychopathy: Affect and Behavior* in Cooke D. J. and Forth A. E. and Hare R. D. (eds), *Psychopathy: Theory, Research and Implications for Society Dordrecht, Netherlands* (Kluwer Academic Publishers1998).

Ianni Francis A. J. and Ianni Elizabeth R., *The Crime Society: Organized Crime and Corruption in America New York* (Meridian Book 1976),1.

Kathari K. R., *Research Methodology: Methods and Techniques* (New Age International Publishers, New Delhi, 2nd ed., 2001, Reprint 2007), 2.

Marion N. E., *Government versus Organized Crime: New Jersey* (Pearson Prentice Hall 2008), 5.

Marx K., *The Communist Manifesto* (International Publishers. New York. 1848, 1932)

Merton R. K., *Social Theory and Social Structure* (Free Press. New York. 1968), 194.

Morrison W., Criminology: Civilization and the New World Order (Routledge Publisher London. 2006).

Obokata T., Transnational Organized Crime in International Law Oxford (Hart Publishing 2010), 14.

Opolot J. S. E., Organized Crime in Africa, Jonesboro (Pilgrimage), 18.

Pfohl S., *Imaged of Deviance and Social Control: A Sociological History* (McGraw Hill, New York. 1994), 113.

Shinder D. L., 2002 'Scene of the Cyber-crime: Computer Forensics Handbook (Syngress Publishing Inc. USA 2022), 88.

Shaw C. R. and McKay H. O., *Juvenile Delinquency and Urban Area* (University of Chicago Press 1972).

Siegel L. J. and Welsh B. C. and Senna J. J., *Juvenile Delinquency: Theory, Practice and Law* (Thomson and Wadsworth. Belmont. 2006).

Shoemaker D. J, *Theories of Delinquency: An Examination of Explanations of Delinquent Behavior* (Oxford University Press. New York. 2005).

Standing A., *Rival Views of Organized Crime* (Pretoria ISS), 66.

Sutherland E. H. and Cressey D. R., *Principles of Criminology* (Lippincott. Philadelphia1995).

Thomas D. and Loader B., *Introduction to Cybercrime; Law Enforcement, Security and Surveillance in the Information Age* in Thomas D. and Loader B. (eds.), *Cybercrime: Law enforcement, Security and Surveillance in the Information Age* (Routledge London. 2000), 3.

Tudor J. K., IS security Architecture: An Integrated Approach to Security in the Organisation. (Auerbach Publications, USA 200).

Turk A. K, *Criminality and Legal Order* (Rand McNally Chicago. 1969).

Wall D., *Cybercrimes and the Internet* in D. Wall (ed.), *Crime and the Internet* (Routledge. London. 2001), 3-7.

Walton T., and Young, *New Criminology* (Routledge & Kegan Paul. London), 41-61.

Walton T. and Young, *'New Criminology London'* (Routledge & Kegan Paul 1973), 41

Williams P. and Savona E. U., (eds) *The United Nations and Transnational organized Crime* London (Frank Cass), 3.

Yar M., *Cybercrime and Society* (2nd edn, Sage Publication Inc. 2013), 58.

JOURNALS

Adesina O. S., 'Cybercrime and Poverty in Nigeria' [2017] (13) (4) *Canadian Social Science,* 19-29.

Adom E. E., Internet Development and Connectivity in Nigeria [2005] (39) (3) *Program electronic library and information system,* 257-268.

Ajayi E. F. G., 'The Impact of Cybercrimes on Global Trade and Commerce' [2016] (2)*'International Journal of Information Security and Cybercrime (IJISC).*

Amaike B, 'Quality of Life of Destitute Older People in Metropolitan Lagos, Lagos State Nigeria' [2011] (ix) *UNILAG Sociological Review (USR),* 6.

Collin B. C., 'The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge' [1996] 11th *Annual International Symposium on Criminal Justice Issues.*

Cowling W., Fighting Organized Crime. *Comment on the Prevention of Organized Crime Bill* 1998 (11 SACJ 350-374), 350.

Dashora K., 'Cyber Crime in the Society: Problems and Preventions' [2011] (3)(1) *Journal of Alternative Perspectives in the Social Sciences,* 240-259

Dewanjee R. and Vyas V., 'Cyber Crime: Critical View' [2013] (6) (14) *International Journal of Science and Research (IJSR)* ISSN, 2319-7064.

Eggleston E. P and Laub J. H., 'The Onset of Adult Offending: A Neglected Dimension of the Criminal Career' *Journal of Criminal Justice,* [2002] (30) (6), 603.

Ehimen O. R. and Bola A, 'Cybercrime in Nigeria' [2010] (3) (1) *Business Intelligence Journal.*

Ellison L. and Akdeniz Y., 'Cyberstalking: The Regulation of Harassment on the Internet' [1998], *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet,* 29-48.

Gerard P. and Broze G, 'Encryption: An Overview of European Policies' [1997] (3)(4). *IT Telecoms and Broadcasting CTLR,* 168.

Gottfredson, M. R., and Hirschi T., *A General Theory of Crime*' (Stanford University Press. 1990), 15.

Hathaway O. and others, 'The Law of Cyber-Attack' [2012] *Faculty Scholarship Series*; 817-885 at 833.

Hirschi T. and Hindelang M., Intelligence and Delinquency: A Revisionist Review' *American Sociological Review* [1977] (42) (4), 571 -587.

Levi M. and others, 'The Implications of Economic Cybercrime for Policing' [2015] *Research Report City of London Corporation.*

Maghu S. and Sehra S. and Bhardawaj A., 'Inside of Cyber Crimes and Information Security: Threats and Solutions' *International Journal of Information & Computation Technology,* [2014] (4)(8), 836.

Maitanmi O. Ogunlere O. and Ayinde S., 'Impact of Cyber Crimes on Nigerian Economy' [2013] (2) (4) *The International Journal of Engineering and Science (IJES),* 45—51.

McGloin J. M. and Pratt T. C. and Maahs J., 'Rethinking the IQ-Delinquency Relationship: A Longitudinal Analysis of Multiple Theoretical Models' *Justice Quarterly* [2004] (21) (3), 603-635.

Moffitt T. E., 'Adolescence-limited and Life-course-persistent Anti-Social Behavior: A Developmental Taxonomy' [1993] (100) (4) *Psychological Review*, 674-701.

Moore M., 'Psychological: Theories of Crime and Delinquency' [2011] (21) *Journal of Human Behavior in the Social Environment* 226-239.

Obidimma E. O. C. and O. Ishiguzo., 'Cybercrime Investigation and Prosecution in Nigeria: The Critical Challenges' [2023] (8) *African Journal of Criminal Law and Jurisprudence (AFJCLJ),* 30.

Okeshola F. B. and Adeta A. K., 'The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria' [2013] (3)(9) *American International Journal of Contemporary Research.*

Olusola M., 'Impact of Cyber Crimes on Nigerian Economy' [2013] (2) (4) *The International Journal of Engineering and Science (IJES),* 45-51.

Omodunbi B., and others, 'Cybercrimes in Nigeria: Analysis, Detection and Prevention' [2016] (1) (1) *FUOYE Journal of Engineering and Technology*, 37-42.

Orji U. J., 'An Inquiry into the Legal Status of the ECOWAS Cybercrime Directive and the Implications of its Obligations for Member States' [2019] (35) (6) *Computer Law and Security Review.*

Rajesh K. G., 'Importance of Cyber Security' [2015] (111) (2) *International* Journal of Computer Applications, 0975-8887.

Saini H. and Rao Y. O. and Panda T. C., 'Cyber-Crimes and their Impacts: A Review' [2012] (2)(2) *International Journal of Engineering Research and Applications* (IJERA), 206.

Short J. F. Jr, 'Criminology: The Chicago School and Sociological Theory' [2002] (37) (2) Journal of *Law and Social Change*, 107-115.

Tade O. and Aliyu I., 'Social Organisation of Cybercrime among University Undergraduates in Nigeria' [2011] (5) *International Journal of Cyber Criminology*, 860–875.

Tappan P., Who is the Criminal? [1947] (12) *American Sociological Review*, 96—102.

Turner J. H. and Marx and Simmel (rev edn), Reassessing the Foundations of Conflict Theory [1975] (53) (4), *Social Forces,* 618-627.

Umaru I., 'The Impact of Cybercrime on the Nigerian Economy and Banking System'. [2019] (36) (12) *NDIC Quarterly.*

Williams G., 'The Definition of Crime: Current Legal Problems' [1955], 107.

Yassir A. and Nayak S., 'Cybercrime: A Threat to Network Security' [2012] (12) (2) *International Journal of Computer Science and Network Security.*

Zembroski D., 'Sociological Theories of Crime and Delinquency' *Journal of Human Behavior in the Social Environment,* [2011] (21), 240-254.

OTHER SOURCES

Flexner S. B., 2010 'Oxford English Dictionary' (3rd edn, Oxford University Press, 2010).

Gordon Stowell (ed), Waverly Encyclopedia of Fact: (Waverley Book Company. 1953).

Imhabekai Maryclaret Osi, Prevention and Control of Cybercrime in Nigeria: Problems, Issues and Strategies (A Dissertation submitted to the School of Postgraduate Studies, University of Ibadan, Zaria in Partial fulfillment for the award of Master of Laws (LLM), 2018).

McCabe S, 'Crime' in D. Walsh and A. Poole (eds), A Dictionary of Criminology; (Routledge and Kegan Paul Publishers London. 1983), 49-52 at 49.

Scott H., 'Concise Encyclopedia of Crime and Criminals London' (Andre Deutsch Ltd. 1961), 84-85.

Scott J., 'Oxford Dictionary of Sociology' (3rd edn, Oxford University Press, 2005).

The New Encyclopedia Britannica, London: [1985] (5) Encyclopedia Britannica.

WEBSITES

African Union Convention on Cyber-security and Personal Data. <https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html.>. Accessed 1st March 2024.

CRS Report for Congress on the Economic Impact of Cyber-Attacks. [2004] <www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf> Accessed 20th November 2023.

Detailed History of internet in Nigeria. < http://innovative.ng/detailed-history-of-internet-in nigeria/>. Accessed 28th January 2024.

IBM survey (published 2006). <www.03.ibm.com/industries/consum erproducts/doc/ content/news/pressrelease/1540939123.html>. Accessed 20th November 2023.

Internet Crime Complaint Centre (IC3).< https://www.ic3.gov>. Accessed 1st March 2024.

Internet World Statistics, Internet Users Statistic for Africa and Internet Penetration in Africa as at 31st January 2017 <www.internetwordstats.com/stats1.html>. Accessed 20th November 2023.

Interpol on International Cybercrime. <www.interpol.int/Crime-areas/Cybercrime Cybercrime>. Accessed 20th November 2023.

The difference between computer crime and cybercrime <https://www.coursehero.com/file/p73g3ob/Difference-Between-Cybercrime-and-Computer-Crime-is-the-term-cybercrime-refers/>. Accessed 3rd February 2024.

Way Back History of Internet in Nigeria. <https://vtpass.com/blog/index.php/2023/05/02/wayback-history-of-internet-in-nigeria/#:~:text=The%20first%20ISP%20was%20founded,services%20to%20already%20burgeoning%20market>. Accessed 29th December 2023.

Ajayi E. F. G., 'The Impact of Cybercrimes on Global Trade and Commerce [2016] (2)*' International Journal of Information Security and Cybercrime (IJISC),* America's Cyber Defense Agency, 'combatting Cyber-crime' <https://www.cisa.gov/combatting-cyber-crime>. Accessed 1st March 2024.

Akinleye A., Reuters, 'Forty Percent of Nigerians live below the poverty line: Report' [2020].<https://www.aljazeera.com/economy/2020/5/4/forty-percent-of-nigerians-live-below-the-poverty-line-report >. Accessed 4th February 2024.

Bello A. T., 'Anatomy of Cybercrime in Nigeria: The Legal Chronicle [2017]. http://www.newsfromafrica.org/newsfromafrica/articles/art_14335.html . Accessed 1st March 2024.

Benfield R. and Dockar A., 'Cyber-attack: Is your Property Adequately Protected' [2018]. <https://hsfnotes.com/realestatedevelopment/2018/05/17/cyber-security-is-your-property-adequately-protected/>. Accessed 4th February 2024.

Botnets, Cybercrime and Cyber terrorism: (2008) Vulnerabilities and Policy Issues for Congress Order Code <http://fas.org/sgp/crs/terror/RL32114.pdf>. Accessed 4th February 2024.

Cardiff University, 'The Implications of Economic Cybercrime for Policing' [2015]. City of London Corporation. <www.cityoflondon.gov.uk/business/researchpublications>. Accessed 1st March 2014.

Chitadze N., 'Global Dimension of Organized Crime and Ways of Preventing Threats at the International Level' [2016] (15) (3) *Connection QJ*, 17-32. <https://doi.org/l0.11610/Connectjons.15.3.02>. Accessed 3rd February 2024.

Chukwuma O. V., Okolie I. P. and Eneh A. N., 'Automated forensic auditing and fraud control in Nigeria' (2022) *International Journal of Multidisciplinary Research and Growth Evaluation.*<https://www. researchgate.net/publication/ 366544280_Autom ated_forens c_auditing_and_fraud_control_in_Nigeria>. Accessed 1st March 2024

Coffman K. G. and Odlyzko A. M., 'Growth of the Internet' <https://www.scienced I rect.com>. Accessed 3rd February 2024.

Connell M. C. 'Cybercrime and Punishment: Archaic Law Threaten' <www.iwar.org.ukresourcesmcconnell> Accessed 28th December 2023.

Csuri A., Cybercrime is World's Third–Largest Economy [2023] Threat Intelligence. Accessed 4th February 2024. <https://stripeolt.com/knowledge-hub/expert-intel/cybercrime-is-worlds-third-largest-economy>. Accessed 4th February 2024.

Deonandan R., 'Defining poverty: A summary of competing models' [2019] (2) (1) *Journal of Social and Political Sciences,* 17–21.

Donnell L. O., 'Threat List: Nigerian Cybercrime Surged 54 percent in 2018' [2019]. <threatpost.com//vulnerabilities>. Accessed 4th February 2024.

Douwe Korff. 'Cyber Security Definitions: A Selection' <https://www.sbs.ox.ac.uk.>system >files>. Accessed 28th December 2023. Also available on <http://niccs.us-cert.gov./glossary#cybersecurity>.

Ernst & Young LLP 2015 Strategic National Measures to Combat Cybercrime: Perspective and Learning's for India [2015] <https://www.ey.com>vwLUAssest>ey-strategic-national-measures-to-combat-cybercrime.pdf>. Accessed 1st March 2024.

Ewepu G., 2016 Nigeria loses N127bn annually to cyber-crime — NSA available at: <http://www.vanguardngr.com/2016/04/Nigeria-losesn127bn-annually-cyber-crime-nsa/>. Accessed 4th February 2024.

Fan M. and Nunyuie O., 'Investigating the Effects of Cyber Fraud on Customer Trust for Online Shopping: The Ghanaian Setting' [2019] (11) (39), 86-96. <https://core.ac.uk/download/pdf/276531331.pdf >. Accessed 4th February 2024.

Gercke M., 'Understanding Cybercrime: Phenomena, Challenges and Legal Response' <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>. Accessed 20th November 2023.

Hassan A. B. and Lass F. D. and Makinde J., 'Cybercrime in Nigeria: Causes, Effects and the Way Out' [2012] (2) (7) *ARPN Journal of Science and Technology*, 628. < http://www.ejournalofscience.org> Accessed on 30th January 2024.

Iroegbu S., 2016 Nigeria loses over N127bn annually through cybercrime. <http://www.thisdaylive.com/index.php/2016/04/19/Nigeria-loses-over-n127bn annually-through-cybercrime/>. Accessed 29th December 2024.

Jones C. 2015 'How do 'We' Police Cyber' [2015].<serocucybercrimeunit@thamesvalley.pnn.police.uk>. Accessed 1st March 2024.

Kahn R. E. and Cerf V.O., 'What is the Internet (And What Makes It Work) Note XV' <https://www.cnri.reston.va.us/what is internet.html>. Accessed 3rd February 2024. Also available on <http://www.fnc.gov>.

Kaspersky Security Network (KSN). <https://technext24.com/2023/06/07/nigeria-south-africa-kenya-cyber-threats/>. Accessed 28th January 2024.

Legal Brief, E-Law & Management, [2015] (1581) *Cyberlaw & Technology*,1

Lipton D., 'Cyber security: Threats Call for a Global Response' [2020].<https://www.imf.org/en/Blogs/Articles/2020/01/13/blog-cybersecurity-threats-call-for-a-global-response>. Accessed 1st March 2024.

McAfee Inc. 2014 Net losses: Estimating the Global Cost of Cybercrime. <https://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf>. Accessed 4th February 2024.

McGuire M., and Dowling S., 'Cyber Crime Investigation: Making a Safer Internet Space' *Research Report,* 75. <https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf>. Accessed 4th February 2024.

Mukherjee A., 'Difference between Cyber Crime and Conventional Crime' (2023) <https://lawcorner.in/difference-between-cyber-crime-and-conventional-crime-in tabular-form/ >. Accessed 1st of March 2024.

Nigerian Cybercrime Ring's Phishing Tactics Exposed. Infosecurity Magazine (May 2023). See also <https://www.infosecurity-magazine.com>. Accessed 27th February 2024.

Njoku D. O., 'Ranking Countries with fear of Cybercrime in Africa' [2023] ResearchGate <https://www.researchgate.net/figure/Ranking-of-Countries-with-fear-of-Cybercrime-in Africa-Source-World-Bank-Ease-of-Doing fig1 338456129 >. Accessed 4th February 2024.

Nweke O. J., 'The rapid growth of internet fraud in Nigeria, Cause, Effect and Solution' (2014) <https://innertempleoou.wordpress.com/2017/03/07/the-rapidgrowth-of-internet-fraud- in-nigeria-cause-effect-and-solution-by-nweke-oluchi-jacinta/ >, Accessed 4th February 2024.

Oludayo T., 'A Spiritual Dimension to Cybercrime in Nigeria: The 'Yahoo Plus' Phenomenon'.699.<https://www.researchgate.net/publication/272040780_A_spiritual_dimension_to_cybercrime_in_Nigeria_The_'yahoo_plus'_phenomenon> . Accessed 28th January 2024.

Omodunbi B., and others, 'Cybercrimes in Nigeria: Analysis, Detection and Prevention' [2016] (1) (1) FUOYE Journal of Engineering and Technology, 37-42. Also accessed 28thJanuary,2024.<https://www.researchgate.net/publication/320411102_Cybercrimes_in_Nigeria_Analysis_Detection_and_Prevention> Accessed 28th January 2024.

Onuoha U.D. and Ikonne C. N., 'Dealing with the Plague of Plagiarism in Nigeria' [2013] (4) (11). See also <https: //core.ac.uk/download/pdf/234634388.pdf>. Accessed 29th February 2024.

Onuora A. C. and others, 'The Challenges of Cybercrime in Nigeria: An Overview' [2017] (1) (2) *AIPFU Journal of School of Sciences (AJSS),* 6-11. <https://www.researchgate.net/publication/338236273_The_Challenges_of_Cybercrime_inNigeria_An_Overview>. Accessed 4th February 2024.

Organised Crime in Nigeria: A Threat Assessment. [2023]. A research conducted by United Nations Office on Drug and Crime (UNODC). <https://www.unodc.org/conig/uploads/documents/NOCTA_Web_Version_25.09.2023.pdf>Accessed 4th February 2024.

Otieno D., 'Cyber security challenges: The Case of Developing Countries' [2020] <https://www.researchgate.net/publication/346485466_Cyber_security_challenges_T e_Case_of_Developing_Countries>. Accessed 28th January 2024.

Oyewole and Obeta, 'An Introduction to Cyber Crime' (2002) <http://www.crirneresearch.org/articles/-crime>. Accessed 3rd February 2024.

Popov A., 'How COVID-19 Triggered the Digital and E-commerce Turning Point' <https://unctad.org/news/how-covid-19-triggered-digital-and-e-commerce-turning-point>. Accessed 4th February 2024,

Proxy Servers, November 2018. <https://kb.iu.edu/d/ahoo.>. Accessed 1st March 2024.

Ribadu N., 2007. Cyber-Crime and commercial fraud: A Nigerian perspective. Presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL (United Nations Commission on International Trade Law), Vienna, Austria, 9-12 July. <http://www.cnudmi.org/pdf/english/congress/Ribadu_Ibrahim.pdf>. Accessed 29th December 2023.

Richard O., 'Nigeria: Putting the Cybercrime Law to Test in 2016' <http://allafrica.com/stories/201601060369.htmI>. Accessed on 17th January 2024.

Russu C., 'The impact of low cyber security on the development of poor nations' [2022]. <https://www.developmentaid.org/news-stream/post/149553/low-cyber-security-and-development-of-poor-nations >. Accessed 1st March 2024.

Sasu D. D., 'Internet 'Nigeria: online usage Penetration' 2018 to 2027' (2024). <https://www.statista.com/statistics/484918/internet-user-reach-nigeria/>. Accessed 1st of March 2024.

Saunders J. 'Tackling cybercrime – the UK response' [2017] (2)(1) <https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1293117>. Accessed 1st March 2024.

Scottish Center for Crime and Justice Research: *Theories and Causes of Crime.* <http://www.sccjr.ac.uk/work-with-us/courses/Iearning-resources-for-schools/#what-is-crime >. Accessed 3rd February 2024.

Scottish Government, 'Consultation on Proposal for a Cyber Resilience Strategy for Scotland' [2015]. <https://consult.gov. scot/cyber-resilience-policy-team/cyberconsultation/user_uploads/cyber-consultation-june-2015_final.pdf>. Accessed 1st March 2024.

Security & Support Proshare 'Cybercrime in Nigeria', Causes and Effect' [2020]. <www.proshareng.com>. Accessed 8th February 2024.

Shashikala G., 'Problems of Jurisdiction in Cyberspace and its Impact on International and Domestic Laws' [2023] <http://shodhganga.i nflibnet.ac.in/bitstream/10603/113328/5/chapter%20ii.pdf >. Accessed March

Stalans L. J. and Finn M. A., 'Understanding How the Internet Facilitates Crime and Deviance' [2016] (11) (4). *An International Journal of Evidenced-based Research, Policy, and Practice.* Accessed 4th February 2024. <https://www.tandfonline.com/doi/full/10.1080/15564886.2016.1211404>.

Taylor S., 'VPN: Every about VPN you need to know, [2019]. <https://restoreprivacy.com/vpn > . Accessed March 2024.

Tentena P. 'Tackling the challenges of cybersecurity in Africa' [2014] (2) *Policy Brief, NTIS.* <http://www.uneca.org/sites/default/files/uploads/ntis_policy_brief_1.pdf >. Accessed 1st March 2024.

UK and US Develop New Global Guidelines for AI Security [2022]. = <https://www.ncsc.gov.uk/news/uk-develops-new-global-guidelines-ai-security>. Accessed 1st March 2024.

United Nations International Telecommunication Union Cyber Security. <http://www.itu.int/en/ITU-T/studygrou ps/corn 17/Pages/cybersecurity.aspx>. Accessed 28th December 2023.

United States Cyber Security Awareness Month, it is usually observed every October each year.<https://www.nist.gov/cybersecurity/cybersecurity-awareness month#:~:text=2023%20marks%2020%20Years%20of,safer%20and%20more% 20secure%20online>. Accessed 1st March 2024.

University of Maryland, 'University College Introduction to Cyber Security' <www.umuc.edu.academic-programs/cyber-security?about.cfm>. Accessed 28th January 2024.

Waibel M., and T. Malone, '*Constitutional Protections Afforded to Individuals Subject to an Extradition Request*' [2017] (8)(1) *University of Cambridge Faculty of Law Legal Studies Research Paper Series on SSRN.*<https://www.law.cam.ac.uk/ press/news/2017/01/legal-studies-research-paper-series-vol-8-no-1>. Accessed 1st March 2024.

Weimann G., Cyber 'Terrorism: How Real is the Threat?' [2014] Unite States Institute of Peace. *Special Report 119.* <https://www.usip.org/sites/default/files/sr119.pdf>. Accessed 4th February 2024.